Les mesures d'importance fiabilistes issues des Etudes Probabilistes de Sûreté nucléaires : *contrôle des incertitudes et nouvelles applications pour l'aide à la décision.*

NICOLAS DUFLOT

19 juin 2007

Directeur de thèse : Christophe Bérenguer, Laurence Dieulle

Jury :

Rapporteurs	Marko Čepin
	Antoine Rauzy
Examinateurs	Antoine Grall
	Nikolaos Limnios
	Dominique Vasseur
	Enrico Zio

Table des matières

Introduction générale

1 Pourquoi et comment estimer les risques liés à une centrale nucléaire

En sa qualité d'exploitant nucléaire, l'entreprise EDF a l'obligation de veiller à ce que son activité ne fasse pas peser de risque significatif sur le public, notamment en termes de radioprotection. Pour pouvoir concevoir des centrales nucléaires sûres, une approche déterministe de conception a été adoptée. Elle consiste à dimensionner les installations à partir d'un petit nombre de scénarios majorants. L'hypothèse est alors faite que les systèmes de sécurité permettant de faire face à des accidents majeurs sont aussi en mesure de traiter des accidents de moindre importance. La conception de ces systèmes incorpore de plus les bonnes pratiques (par exemple, la valeur des marges de sécurité) observées dans chaque domaine. Cependant, ces études préliminaires à la mise en exploitation d'une nouvelle centrale ne permettent pas de connaître le niveau de risque de celle-ci, ni les séquences accidentelles les plus probables. Ainsi, Vesely souligne dans [90] que "*l'identification des séquences accidentelles et la quantification de leur probabilité n'était pas faite de manière systématique avant 1975*".

Les études probabilistes de sûreté (EPS) de référence ont donc été développées pour permettre de déterminer le risque de référence. Celui-ci se définit comme la probabilité d'occurrence, pour une centrale donnée, de "conséquences inacceptables" telles que la fusion du cœur ou le rejet d'éléments radioactifs dans l'environnement. Le terme "de référence" signifie que la centrale est initialement dans son état nominal.

La première EPS mise au point par EDF représentait de manière semi-dynamique le fonctionnement de chaque système. Elle permettait de calculer les données suivantes :
- la fréquence de fusion du cœur,
- la probabilité de défaillance de chaque système en fonction du temps,
- la probabilité de chaque séquence accidentelle.

Cette première EPS de référence était initialement calculée avec le logiciel LESSEPS. Les applications des EPS se développant, il est ensuite apparu utile de pouvoir exprimer le risque à partir de coupes minimales d'événements élémentaires, c'est-à-dire en termes de mode de défaillance spécifique de composants spécifiques pour pouvoir connaître l'importance de chaque événement. LESSEPS a donc été remplacé par le logiciel booléen RiskSpectrum Windows (RSW). Comme d'autres logiciels booléens dédié aux EPS, celui-ci permet, en couplant des arbres d'événements et des arbres de défaillances, d'élaborer une fonction de structure approchée modélisant l'occurrence des "conséquences inacceptables". Il propose une modélisation un peu moins fine que LESSEPS (pas de prise en compte de la dynamique temporelle des séquences accidentelles) mais produit une expression du risque sous forme de coupes minimales. Cela permet une meilleure compréhension des composantes du risque et simplifie ainsi l'aide à la décision. RSW a tout d'abord été utilisé pour générer les informations suivantes :

- la fréquence de fusion du cœur,
- les coupes minimales de référence,
- la probabilité de chaque séquence accidentelle.

Comme le souligne Fleming dans le NUREG 6813 [49], depuis une décennie, l'utilisation des EPS s'est orientée de plus en plus vers leur application à l'aide à la décision (démarche de type "Risk Informed"). Dans le cadre de ce type de démarches, les modèles EPS sont utilisés pour étudier, au moyen d'indicateurs adéquats, l'importance des événements qui y sont modélisés vis-à vis du risque. Ces indicateurs, appelés facteurs d'importance ou mesures d'importance, doivent notamment permettre de hiérarchiser les problèmes en fonction de leur gravité et donc aider à la prise de décision. Une telle réorientation du domaine d'application des modèles EPS implique de nouveaux enjeux en termes de maîtrise des incertitudes.

2 Contexte de l'étude

Notre étude s'inscrit dans un cadre industriel, celui de l'exploitant nucléaire EDF. Elle prend donc en compte un certain nombre de contraintes et impératifs, tant techniques qu'économiques, qui sont celles des centres d'ingénierie, principaux destinataires des études et méthodes développées par la direction R&D d'EDF.

Le premier impératif est celui de la qualité des solutions, gage de sûreté. En effet, les conclusions des études et les propositions faites sur leur fondement peuvent conduire à des prises de décision qui ont un impact potentiel sur le risque lié à l'exploitation des centrales. Une approche de type "essai / erreur" est donc exclue. On ne peut pas, comme on le ferait par exemple en laboratoire, procéder par "tâtonnements". Une fois que le résultat d'une étude EPS est validé, la solution proposée est mise en œuvre et il est alors difficile de le remettre en cause. Elle doit d'emblée être adaptée et, dans le pire des cas, ne pas dégrader la sûreté.

Le deuxième ensemble d'impératifs est étroitement lié à l'ergonomie des solutions et à l'intérêt qu'elles suscitent auprès de leurs destinataires. Ainsi, en plus d'être innovantes et adaptées au besoin, elles doivent pouvoir être mises en œuvre de manière rapide et aisée, sans rencontrer de difficultés techniques (liées en particulier aux matériels informatiques communément utilisés) et en permettant une "prise en main" facile. Cette relative simplicité d'emploi est d'autant plus importante que les utilisations sont fréquentes. Au-delà de la mise en œuvre des solutions, il importe de veiller à ce que les outils et méthodes proposés avec ces solutions soient suffisamment clairs pour que les utilisateurs finaux puissent se les approprier. Leurs principes de fonctionnement doivent pouvoir être compris par leurs utilisateurs, de manière à ce que ceux-ci en connaissent les éventuelles limites en termes de capacités et de précision, et qu'ils puissent le cas échéant les adapter à leurs besoins. D'une manière plus générale, il s'agit de susciter l'adhésion des "bénéficiaires" des études réalisées. Ceci passe en premier lieu par l'analyse et la prise en compte de leurs attentes. Dans un contexte industriel, la solution proposée n'est jugée pertinente que dans la mesure où elle trouve une application pratique et réelle dans les missions des ingénieurs et techniciens de l'entreprise.

Le troisième ensemble d'impératifs est de nature économique. Au vu du coût d'élaboration d'un modèle EPS, il est clair que les principes de base qui supportent ces modélisations (modèle booléen représenté au moyen d'arbres de défaillances et d'arbres d'événements) ne peuvent pas être remis en cause. De même, les solutions que nous nous proposons d'apporter doivent impliquer le moins de modifications des modèles possible. En effet, chaque modification représente un coût en main d'œuvre d'autant plus élevé qu'elles est réalisée par des ingénieurs expérimentés et peu nombreux. Une autre implication de cette contrainte économique est la nécessité d'utiliser RSW : les modèles EPS ont été développés pour s'adapter aux spécificités algorithmiques de ce logiciel. Les développements nécessaires au portage des modèles EPS d'EDF sous une autre

application informatique ont un coût prohibitif. Toutes les méthodes que nous serons amenés à développer doivent donc être compatibles avec l'utilisation de RSW.

3 Enjeux de la thèse : maîtriser les incertitudes et proposer de nouvelles applications

Dans un contexte industriel tel que celui d'EDF, les indicateurs de risque proposés doivent pouvoir être calculés de manière précise et économique. Le premier problème à résoudre est donc le développement de modes de calcul permettant d'obtenir ces indicateurs simplement, rapidement et automatiquement, tout en maximisant la précision des résultats. Pour ce faire, il faut identifier et réduire, dans la mesure du possible, les différentes causes d'incertitudes sur les mesures d'importance.

En effet, l'objectif initial des modèles EPS d'EDF est de calculer le risque de référence. Des simplifications de modélisation et algorithmiques n'ayant pas d'impact sur ce calcul ont donc été mises en œuvre. Si l'on souhaite estimer l'importance des événements contenus dans ces modèles, il faut vérifier que ces simplifications, justifiées dans le cadre du calcul du risque de référence, n'entraînent pas d'incertitudes significatives lors du calcul des mesures d'importance. Nos travaux s'attachent donc, dans un premier temps, à établir les modalités d'un calcul d'indicateur de risque qui ne soit pas entaché d'incertitudes préjudiciables à la justesse du résultat. C'est, d'après Fleming (NUREG 6813 [49]), l'une des limitations majeures à une plus large utilisation des EPS dans l'aide à la prise de décision.

Une fois que les modèles ont été rendus capables de calculer un indicateur de risque sans une trop grande incertitude, nous envisageons l'application de ces indicateurs non plus seulement à des événements élémentaires, mais aussi à des événements composés, tels que la défaillance d'un système, la perte ou la non-existence d'une fonction. Leur champ d'application pourra alors être étendu à la gestion des indisponibilités, ce qui permettra entre autres de minimiser l'impact des arrêts pour maintenance sur les coûts et la sûreté.

Enfin, l'utilisation de ces indicateurs pour optimiser la conception de nouvelles centrales est étudiée et une démarche d'utilisation des indicateurs de risque pour l'aide à la conception est proposée.

Chapitre 1

Les EPS et leurs indicateurs de risque

1 Les études probabilistes de sûreté (EPS)

1.1 Ce que mesurent les EPS

D'après l'AIEA [5], l'objectif de la sûreté nucléaire est que "*chaque individu, la société dans son ensemble et l'environnement soient protégés de tout risque radiologique lié aux centrales nucléaires en établissant et en conservant un confinement efficace*".

Pour assurer ce confinement, des barrières physiques sont mises en œuvre. Le Mémento de la sûreté nucléaire [39] définit ces barrières comme "*des obstacles physiques à la dispersion des produits radioactifs*". Dans les centrales actuelles de type Réacteur à Eau sous Pression (REP), il existe trois barrières physiques : la gaine des crayons de combustible, le circuit primaire et l'enceinte de confinement. Le terme "barrière" ou encore "barrière physique" sera réservé à la désignation de ces "*obstacles physiques*".

On distingue les EPS en fonction du ou des événements redoutés qu'elles visent à quantifier. Ainsi, le but des EPS de niveau 1 est d'étudier, sur un cycle du combustible (12 ou 18 mois), la probabilité ou la fréquence de fusion de la première barrière suite à une défaillance de son refroidissement. L'événement redouté sera donc l'événement "$FUSION$" (des gaines de combustible).

Dans une EPS de niveau 2, le but est d'étudier, sur un cycle du combustible, la probabilité ou la fréquence de fuite de ces trois barrières en même temps. Les événements redoutés seront des rejets trop importants de matières radioactives dans l'environnement. On pourra, par exemple, estimer la fréquence de rejets précoces (avant 24 heures) massifs et non filtrés, la fréquence de rejets non filtrés après 24 heures, et enfin la fréquence de rejets filtrés après 24 heures.

Dans une EPS de niveau 3, on étudie les conséquences d'une fuite de ces trois barrières en même temps sur la population et l'environnement. Les événements redoutés seront donc des décès, des cas de cancer, une pollution de l'environnement ou encore le coût financier global pour la société.

De manière générale, quelle que soit l'EPS concernée (niveau 1 ou niveau 2), on considérera qu'elle a pour but d'estimer, sur un cycle du combustible et pour une centrale donnée, la probabilité ou la fréquence d'atteinte de conséquences inacceptables, CI (fusion du cœur pour les EPS de niveau 1 ou rejets précoces et massifs pour les EPS de niveau 2). On étudiera alors la fréquence ou la probabilité de l'événement CI en fonction de la probabilité et de la fréquence d'événements élémentaires. On la notera $Q(CI)$ si c'est une fréquence et $P(CI)$ si c'est une probabilité. La probabilité (ou la fréquence) d'atteinte de conséquences inacceptables sera désignée, par la suite, comme étant le "risque de référence", noté R. Il correspondra donc à la probabilité (ou la fréquence) d'occurrence de l'événement CI sur un an.

Le risque est communément défini comme [96] : “ *La mesure d’un danger associant une mesure de l’occurrence d’un événement indésirable et une mesure de ses effets et conséquences* ”. L’unité du risque de référence dépend de l’EPS utilisée c’est à dire des conséquences de l’occurrence de l’événement CI. Pour une EPS de niveau 3, par exemple, on pourra parler en euros par an [1].

1.2 Fondements théoriques des EPS

Cette section présente les fondements des modèles EPS, de la description du comportement de la centrale à l’étude jusqu’aux calculs du risque de référence. Pour ce faire, nous verrons tout d’abord ce qu’est une fonction de structure, puis comment le fonctionnement de l’installation est modélisé et comment de ces modèles on obtient la fonction de structure correspondant à l’événement CI. Enfin, le mode de calcul du risque de référence à partir de cette fonction de structure sera présenté.

1.2.1 Définition des modèles booléens

Le but des EPS est de quantifier la probabilité ou la fréquence d’un événement redouté (CI) exprimé au moyen d’une fonction booléenne appelée fonction de structure. Une fonction de structure exprime l’occurrence d’un événement composé comme une combinaison logique de l’occurrence d’événements élémentaires, encore appelés événements de base et notés EB.

Dans les modèles EPS d’EDF, la fonction de structure $\Phi\left(\underline{e}\right)$ décrit l’atteinte de conséquences inacceptables au moyen d’un vecteur d’état $\underline{e}$ rassemblant l’ensemble des événements de base.

$$\Phi\ :\ \{0;1\}^n \to \{0;1\}\ \text{ avec } \underline{e} = (e_1, e_2, \ldots, e_n) \in [0;1]^n$$

La fonction Φ est une fonction booléenne des variables booléennes e_i telle que si $\Phi\left(\underline{e}\right) = 1$, alors l’événement “atteinte de conséquences inacceptables”(CI) est réalisé et si $\Phi\left(\underline{e}\right) = 0$, alors l’événement “atteinte des conséquences acceptables”(CA) est réalisé ($CA = \overline{CI}$). Le vecteur d’état $\underline{e}$ exprime l’état de chaque événement élémentaire, encore appelé événement de base (réalisé ou non réalisé), qui est tel que :

$$e_i = \begin{cases} 1 \text{ si l'}EB_i\ (EB_i) \text{ est réalisé} \\ 0 \text{ si l'}EB_i\ (EB_i) \text{ n'est pas réalisé } (\overline{EB_i} \text{ est réalisé}) \end{cases}$$

avec $\overline{EB_i}$ l’événement “NON EB_i” qui correspond à la non-occurrence de l’EB_i.

1.2.2 Construction des modèles EPS

Comme on l’a vu précédemment, l’objectif d’une EPS est de définir la probabilité (ou la fréquence) d’un événement redouté (CI) sur un cycle du combustible. Pour cela, la démarche consiste à répertorier toutes les “façons” possibles d’arriver à cet événement, puis à en déterminer la probabilité (ou la fréquence).

La première étape de cette démarche consiste à répertorier tous les événements initiateurs qui peuvent initier une séquence accidentelle conduisant à l’occurrence de l’événement CI. Un événement initiateur est un événement qui, si aucun système de sauvegarde ni aucune action de sauvegarde ne sont mis en œuvre, entraîne l’occurrence de l’événement CI. L’un des enjeux importants pour la qualité du modèle EPS est de n’oublier aucun initiateur lorsqu’on les répertorie. Ainsi, tous les événements pouvant entraîner l’occurrence de l’événement CI doivent être envisagés.

La seconde étape consiste à modéliser la ou les réponses possibles de la centrale nucléaire (en y incluant les moyens techniques et humains) à ces événements initiateurs. On définit donc la

ou les séquences d'événements en tête pouvant partir d'un initiateur pour arriver à l'occurrence de conséquences inacceptables (l'occurrence de l'événement CI). Pour cela, on regardera au moyen d'un arbre d'événements les différentes missions de sauvegarde, encore appelées "événements en tête", qui peuvent être mises en œuvre pour maîtriser les conséquences de l'occurrence d'un initiateur. Ainsi, à chaque séquence accidentelle, on associera une conséquence qui est en général soit l'atteinte de conséquences inacceptables (événement CI), soit l'atteinte de conséquences acceptables (événement CA). On construira donc autant d'arbres d'événements qu'il y a d'initiateurs et chacun de ces arbres contiendra sous forme "d'événements en tête" l'ensemble des missions pouvant avoir un impact sur l'occurrence ou la non-occurrence de l'événement CI, lorsque l'initiateur dont cet arbre fait l'objet s'est produit.

Enfin, la défaillance de chaque mission de sauvegarde est modélisée au moyen d'un arbre de défaillances. Chaque mission de sauvegarde j peut donc être exprimée au moyen d'une fonction de structure $\phi_{mission\ j}\left(\underline{e}\right)$. Les événements élémentaires de cette fonction de structure sont représentés par les feuilles de l'arbre de défaillances correspondant. Ils sont appelés événements de base. Ces événements de base modélisent principalement trois types d'événements :

- un mode de défaillance spécifique d'un composant spécifique (rupture, défaillance à la sollicitation, défaillance en fonctionnement, blocage ouvert/fermé, court-circuit, etc.),
- un événement initiateur (rupture d'une tuyauterie, etc.),
- une erreur humaine (oubli fermé d'une vanne, non-réalisation dans les délais d'une action de sauvegarde, etc.).

A la fin de ce processus, on disposera donc de la liste des initiateurs, des arbres d'événements associés, de l'ensemble des missions de sauvegarde y intervenant et de l'expression, sous forme d'arbre de défaillances, de la fonction de structure $\phi_{mission\ j}\left(\underline{e}\right)$ modélisant l'échec ou le succès de chacune de ces missions.

Exemple : Une brèche dans le circuit primaire aura pour conséquence une perte de réfrigérant. Si cette perte n'est pas compensée par un ajout automatique de réfrigérant (mission de sauvegarde automatique ou "manuelle") ou par un appoint déclenché à partir de la salle de commande (mission de sauvegarde "manuelle"), les conséquences inacceptables seront atteintes. Si l'on étudie ce type d'accident, on considérera donc une brèche comme un initiateur. Sa détection automatique, sa détection en salle de commande, le fonctionnement de l'injection de sécurité et l'appoint manuel constituent des missions de sauvegarde. En effet, elles visent à limiter les conséquences de l'occurrence de l'initiateur. Un arbre d'événements correspondant est donné dans la figure 1.1. La même réalité physique peut aussi être décrite, de manière équivalente, avec l'arbre de la figure 1.2. On voit donc qu'il existe autant d'arbres qu'il y a d'ordres possibles entre les missions de sauvegarde. A une réalité peuvent correspondre plusieurs modèles tous équivalents.

La séquence 2, par exemple, est associée aux conséquences acceptables (CA) et correspond à une trajectoire accidentelle où une brèche sur le circuit primaire est détectée par les automatismes, mais l'injection automatique ne fonctionne pas. Ce sont les opérateurs qui, détectant de la salle de commande la perte de réfrigérant, la compensent par un appoint manuel.

L'exhaustivité recherchée dans la construction des modèles EPS conduit à générer des modèles très volumineux contenant des milliers d'événements de base, des centaines d'arbres de défaillances et d'arbres d'événements.

A partir des fonctions de structure $\phi_{mission\ j}$ de chaque mission et de la structure de chaque arbre d'événement, on peut définir la fonction de structure Φ modélisant l'occurrence de l'événement CI.

Brèche sur le circuit primaire *Initiateur*	Détection automatique de la brèche *Mission 1*	Injection automatique ou manuelle de réfrigérant *Mission 2*	Détection par les opérateurs de la brèche *Mission 3*	Appoint manuel de réfrigérant *Mission 4*	conseq.

Séquence	conseq.
1	CA
2	CA
3	CI
4	CI
5	CA
6	CI
7	CA
8	CI
9	CI

FIG. 1.1 – *Exemple d'arbre d'événements d'une EPS*

Brèche sur le circuit primaire *Initiateur*	Appoint manuel de réfrigérant *Mission* 4	Détection par les opérateurs de la brèche *Mission* 3	Injection automatique ou manuelle de réfrigétant *Mission* 2	Détection automatique de la brèche *Mission* 1	conseq.

Séquence	conseq.
1	CA
2	CA
3	CI
4	CI
5	CA
6	CI

FIG. 1.2 – *Le même arbre exprimé d'une autre manière*

1.2.3 Obtention et expression de la fonction de structure d'une EPS

Quelle que soit la séquence considérée d'un arbre d'événements, on peut obtenir sa fonction de structure à partir des arbres de défaillances modélisant l'échec de chaque mission. Ainsi, la fonction de structure d'une séquence k s'exprime comme :

$$\phi_{seq\ k}\left(\underline{e}\right) = \left(\coprod_{\substack{\text{mission } i \text{ en} \\ \text{échec dans} \\ \text{la séquence } k}} \phi_{mission\ i}\left(\underline{e}\right) \right) \cdot \left(1 - \coprod_{\substack{\text{mission } j \text{ en} \\ \text{succès dans} \\ \text{la séquence } k}} \phi_{mission\ j}\left(\underline{e}\right) \right)$$

avec l'opérateur $\coprod$ correspondant à la somme booléenne (la somme booléenne est telle que l'on ait en particulier $1 + 1 = 1$, $1 + 0 = 1$ et $0 + 0 = 0$).

Si on prend l'exemple de la séquence 6 de l'arbre d'événements de la figure 1.1, pour que $\phi_{seq\,6}\left(\underline{e}\right) = 1$ il faut que les missions 1 et 3 soient en échec, c'est-à-dire $\phi_{mission\,1}\left(\underline{e}\right) = \phi_{mission\,3}\left(\underline{e}\right) = 1$. Mais il ne faut pas que la mission 2 soit réalisée (sinon on serait dans la séquence 9) donc il faut que $\phi_{mission\,2}\left(\underline{e}\right) = 0$.

L'arbre de défaillances équivalent à l'événement "occurrence de la séquence k" (avec k quelconque) contient sous une porte ET l'événement de base "occurrence de l'initiateur" ou l'arbre de défaillances le modélisant, une porte ET regroupant tous les arbres de défaillances modélisant l'échec des missions en échec dans la séquence k, et une porte NON OU regroupant les arbres de défaillances modélisant l'échec de toutes les missions dont on sait qu'elles sont en

succès dans la séquence k.

Par exemple, l'arbre de défaillances équivalent à la séquence 3 de l'arbre d'événements de la figure 1.1 est celui donné dans la figure 1.3.

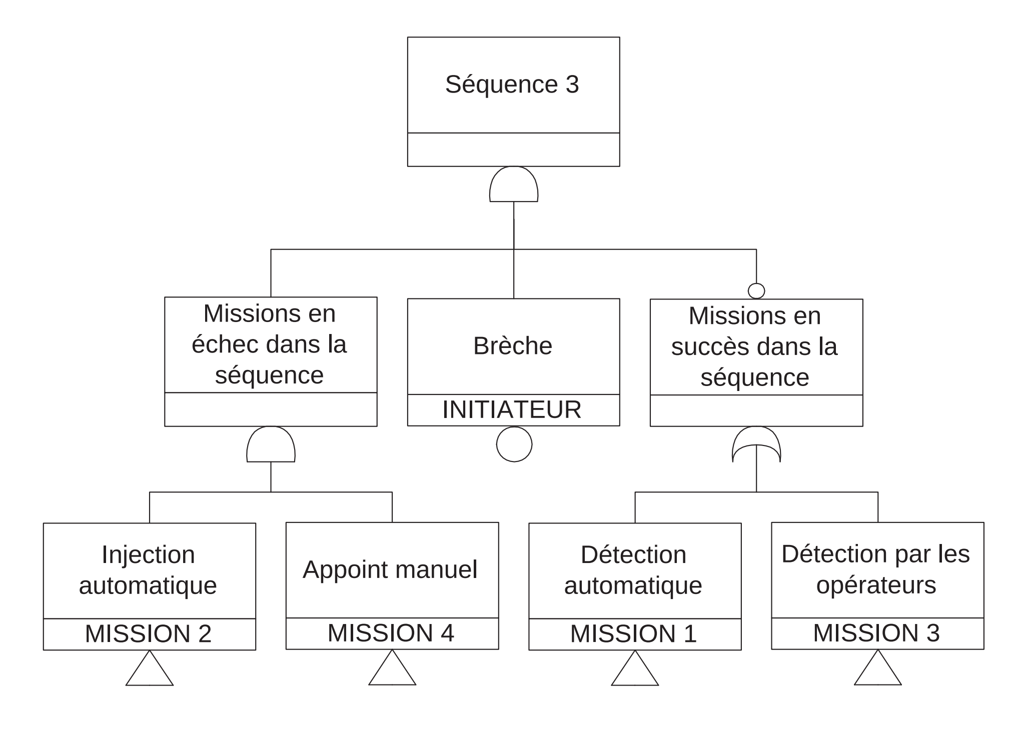


FIG. 1.3 – *Arbre de défaillances équivalent à la figure 1.1*

La fonction de structure correspondant à l'événement "atteinte de conséquences inacceptables" s'obtient en faisant la somme booléenne des fonctions de structure des séquences associées aux conséquences inacceptables :

$$\Phi\left(\underline{e}\right) = \coprod_{\substack{séquence\ k \\ associée\ à\ CI}} \phi_{seq\ k}\left(\underline{e}\right)$$

L'arbre de défaillances équivalent à l'événement CI est un arbre qui regroupe sous une porte OU tous les arbres de défaillances modélisant des séquences associées à l'événement CI.

Par exemple, l'arbre de défaillances équivalent à l'événement CI, si on ne considère que l'arbre d'événements de la figure 1.1, est celui donné dans la figure 1.4.

Ainsi, à partir de l'occurrence ou de la non-occurence de chaque événement de base, on arrive à connaître le succès ou l'échec de chaque mission, puis de chaque séquence, et enfin l'atteinte ou la non-atteinte de conséquences inacceptables. Toutefois, la taille de la fonction de structure d'une EPS peut être telle qu'elle ne puisse pas être exprimée entièrement. La construction de la fonction de structure présentée dans cette section est une construction théorique. En pratique, cette fonction booléenne sera donc simplifiée.

1.2.4 Déterminer la probabilité d'occurrence de l'événement redouté

Hypothèses principales

La quantification de la probabilité d'occurrence de l'événement CI modélisé par la fonction de structure d'une EPS repose sur plusieurs hypothèses :

a. les événements de base sont indépendants,

b. la fonction de structure Φ exprimant l'occurrence de l'événement CI, à partir de l'oc-

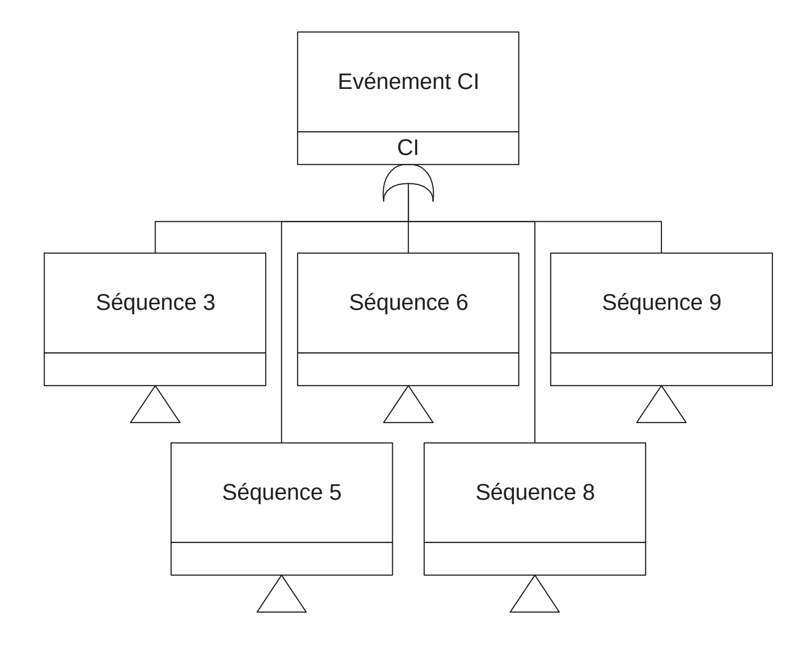


FIG. 1.4 – *Occurrence de l'événement CI telle qu'elle est décrite dans la figure 1.1*

currence des événements de base, est cohérente[1]

c. quel que soit le scénario accidentel considéré, les séquences accidentelles ne sont étudiées que sur les 24 heures suivant l'occurrence de l'initiateur.

Quantification des événements de base

De la première hypothèse (hypothèse a.), on déduit que la probabilité d'occurrence de chaque événement de base ne varie pas, quel que soit l'état des autres événements. Elle peut donc être calculée séparément, sans prendre en compte les autres événements.

Chaque EB appartient à l'une des six catégories suivantes, au sein desquelles on peut définir une règle de calcul de la probabilité d'occurrence :

1. Pour les EB modélisant la défaillance en fonctionnement des matériels sollicités uniquement lors de la gestion d'un initiateur (défaillance en fonctionnement d'une pompe par exemple), chaque probabilité d'occurrence est calculée sur 24 heures (troisième hypothèse) en supposant que leur taux de défaillance (noté λ_i), issu du retour d'expérience (REX), est constant. Cette hypothèse de constance des taux de défaillance implique qu'on est face à un processus sans mémoire et que la probabilité d'occurrence d'un EB_i se calcule comme : $P(EB_i) = 1 - \exp(-\lambda_i \cdot t)$ avec $t = 24h$ et $\lambda_i = constante$.

2. Pour les EB modélisant des défaillances à la sollicitation, chaque probabilité d'occurrence est caractérisée par une probabilité de refus de démarrage, d'ouverture, etc., issue du REX.

3. Pour les EB modélisant des erreurs humaines associées à des actions de conduite nécessaires à la gestion d'un initiateur (non-isolation de l'injection de sécurité lors d'une descente en pression par exemple), chaque probabilité d'occurrence est déterminée à partir de l'application de la méthode MERMOS [73].

4. Pour les EB modélisant des erreurs humaines pré-accidentelles réalisées avant l'occurrence de l'initiateur et impactant des matériels nécessaires à sa gestion (oubli fermé d'une vanne,

[1] Pour la définition de la cohérence d'une fonction de structure, se reporter à la section 2.1.2 du chapitre 1 page 29.

mauvais remontage d'un organe de sécurité, etc.), chaque probabilité d'occurrence est calculée à partir de la méthode FH7 [68] (fortement inspirée de [82]).

5. La probabilité d'occurrence des initiateurs modélisés au moyen d'un unique événement de base, noté $EB_{init,i}$ (événement occurrence d'une brèche entre 2 et 4 pouces par exemple), est calculée à partir du REX ou, en l'absence de REX, à partir d'avis d'experts. Elle correspond à la probabilité d'occurrence de l'initiateur considéré sur la durée du ou des états du réacteur dans lesquels il peut se produire durant un cycle (en puissance, en arrêt à chaud, en arrêt pour rechargement, etc.).

   Dans certains modèles, l'occurrence des initiateurs est exprimée au moyen de fréquences notées f_i avec i allant de 1 à k (k étant le nombre d'initiateurs). En effet, on peut considérer qu'un initiateur peut se produire plusieurs fois sur un cycle du combustible. La fréquence d'occurrence d'un initiateur, telle que $Q\,(EBinit, i) = f_i$, correspond alors au nombre moyen d'occurrences de l'initiateur durant un cycle.

6. La probabilité d'occurrence de certains initiateurs est calculée à partir d'un arbre de défaillances. Dans ce cas, la probabilité d'occurrence des EB qui modélisent dans cet arbre une défaillance en fonctionnement est toujours calculée à partir de leur taux de défaillance issu de l'analyse du REX, mais sur une durée qui est celle sur laquelle l'initiateur peut se produire et non plus sur 24 heures. Par exemple, la probabilité d'occurrence d'un initiateur modélisant la perte d'un système en fonctionnement toute l'année sera calculée à partir de l'arbre de défaillances modélisant la perte de ce système en considérant une durée d'un an.

La classification des EB par catégories et les modes de calcul associés sont présentés par Gallois dans [54]. Pour un aperçu général de la prise en compte des erreurs humaines on peut se référer à [53].

Outil de la quantification : les coupes

De l'hypothèse de cohérence, on déduit que l'événement CI peut être exprimé au moyen de coupes minimales [96]. Une coupe est un événement qui s'exprime comme l'intersection d'événements de base et dont l'occurrence implique celle de l'événement CI.

Une coupe minimale est "*une coupe qui ne contient aucune autre coupe*" [96]. Par la suite, on ne parlera plus que de coupes minimales, que l'on notera CM. On a donc

$$CI = \bigcup_i CM_i \text{ avec } CM_i = \bigcap_{EB_j \in CM_i} EB_j$$

L'hypothèse d'indépendance des EB implique en particulier que la probabilité des EB d'une coupe reste inchangée quel que soit l'état (réalisé ou non) des autres EB. On en déduit que la probabilité d'une coupe reste inchangée quel que soit l'état des autres EB non contenus dans la coupe. On en déduit de plus que la probabilité d'une coupe peut être calculée comme le produit des probabilités d'occurrence des événements de base qui la composent :

$$P\,(CM_j) = \bigcap_{EB_i \in CM_j} P\,(EB_i)$$

Le risque de référence, c'est-à-dire la probabilité d'atteinte de conséquences inacceptables, s'exprime alors comme :

$$R = P\,(CI) = P\,(\Phi\,(\underline{e}) = 1) = P\left(\bigcup_i CM_i\right)$$

Les coupes correspondant à l'événement CI sont appelées coupes de référence car elles servent au calcul du risque de référence.

Comme on l'a vu précédemment, dans les EPS d'EDF, les initiateurs sont mutuellement exclusifs. Le risque de référence $(P(CI))$ correspond donc à la somme des probabilités de l'événement CI considéré dans chaque arbre d'événements. On a alors :

$$P(CI) = P\left(\bigcup_i CM_i\right) = \sum_{i=1}^{nb\ initiateurs} P(EB_{init,i}) \cdot P\left(\left(\bigcup_{EB_{init,i} \in CM_j} CM_j\right) / EB_{init,i}\right)$$

Le risque de référence est donc calculé comme le produit de la probabilité d'occurrence d'un des événements initiateurs par la probabilité d'échec des missions de sauvegarde prévu pour en limiter les conséquences.

Si l'on considère que les initiateurs peuvent se produire plusieurs fois dans un même cycle, on exprime leur occurrence au moyen d'une fréquence f_i et on retrouve l'expression rappelée par Vaurio dans [89] :

$$Q(CI) = Q\left(\bigcup_i CM_i\right) = \sum_{i=1}^{nb\ initiateurs} f_i \cdot P\left(\left(\bigcup_{EB_{init,i} \in CM_j} CM_j\right) / EB_{init,i}\right)$$

avec f_i la fréquence de l'initiateur i (avec f_i à valeur dans $\mathbb{R}^+$). Le risque de référence correspond alors à la somme des fréquences d'occurrence de CI dans chaque arbre d'événements. Chaque terme de cette somme correspond au produit de la fréquence d'occurrence, sur un cycle, de l'initiateur i par la probabilité d'occurrence de l'événement CI sachant l'occurrence de l'événement $EB_{init,i}$.

Par la suite et pour simplifier les notations, on considérera toujours que les initiateurs sont modélisés au moyen d'une probabilité d'occurrence, comme tous les autres EB. Notre risque de référence correspondra alors à la probabilité d'occurrence de conséquences inacceptables sur un cycle pour une centrale donnée.

Les modèles booléens mis en œuvre à EDF ne prennent pas en compte l'ordre d'occurrence des événements. La notion de temps est négligée dans la mesure où on néglige le fait qu'un événement puisse en déclencher un autre. Ainsi, si suite à une brèche, l'injection automatique défaille au bout de 15 heures, on ne devrait estimer la probabilité de défaillance de l'appoint manuel que sur les 9 heures restantes. Pourtant, la probabilité de défaillance de ces deux systèmes sera calculée sur 24 heures. C'est à dire que l'on calculera la probabilité que le premier système soit défaillant au bout de 24 heures et la probabilité que le second système soit défaillant (au bout de 24 heures) sachant que le premier est tombé en panne à $t = 0$. On majore donc leur probabilité de défaillance.

Algorithmes de quantification à partir des coupes

Pour calculer la probabilité de l'union d'un ensemble de n événements, on doit effectuer un développement de Sylvester-Poincaré :

$$P\left(\bigcup_{i=1}^n E_i\right) = \sum_{i=1}^n P(E_i) - \sum_{i \neq j} P(E_i \cap E_j) + \cdots + (-1)^{n-1} \cdot P\left(\bigcap_{i=1}^n E_i\right)$$

En première approximation, on peut effectuer un développement de Sylvester-Poincaré limité à l'ordre k (avec k compris entre 1 et n), qui s'exprime comme :

$$P\left(\bigcup_{i=1}^n E_i\right) \approx \sum_{i=1}^n P(E_i) - \sum_{i \neq j} P(E_i \cap E_j) + \cdots + (-1)^{k-1} \cdot \overbrace{\sum_{i \neq j \neq \cdots \neq k} P(E_i \cap E_j \cap \cdots \cap E_k)}^{\text{toutes les intersections de } k \text{ événements différents}}$$

Selon que $(-1)^{k-1}$ est positif ou négatif, il s'agit d'un majorant ou d'un minorant de $P\left(\bigcup_{i=1}^n E_i\right)$. Plus la valeur de k est proche de n, plus l'approximation est fine.

Grâce à l'hypothèse d'indépendance des événements, on peut calculer la probabilité exacte de chaque coupe au moyen d'un simple produit des probabilités d'occurrence de chaque EB de la coupe. Pour calculer le risque de référence à partir des coupes de référence, on doit, en revanche, utiliser un développement de Poincaré. En effet, puisque les coupes de référence ne sont pas disjointes, leurs intersections ne sont pas vides et il faut donc calculer la probabilité d'occurrence de l'événement CI sur un cycle au moyen d'un développement de Sylvester-Poincaré complet (c'est-à-dire un développement à l'ordre n avec n le nombre de coupes minimales correspondant à l'événement CI). Dans les faits, CI est exprimé à partir de plusieurs centaines de millions de coupes. Ce développement complet est donc, en pratique, impossible à mettre en œuvre.

Le développement de Sylvester-Poincaré à l'ordre 1 du risque à partir de ces coupes nous donne un majorant du risque. Le développement de Sylvester-Poincaré à l'ordre 2 du risque à partir de ces coupes nous donne un minorant du risque. On a donc :

$$\underbrace{\sum_{i=1}^{n}\left(P\left(CM_i\right)-\sum_{\substack{j=1\\ i\neq j}}^{n}P\left(CM_i\cap CM_j\right)\right)}_{\text{Sylvester-Poincaré à l'ordre 2}}\leq P\left(CI\right)\leq \underbrace{\sum_{i=1}^{n}P\left(CM_i\right)}_{\text{Sylvester-Poincaré à l'ordre 1}}$$

Le développement de Sylvester-Poincaré à l'ordre 1 est proche de la vraie valeur du risque si l'hypothèse des événements rares (énoncée ci-dessous) est validée [96]. Puisqu'elle est valide dans nos EPS, le risque est estimé à partir de la somme des probabilités d'occurrence des coupes minimales.

$$\underbrace{P\left(CI\right)\approx\sum_{i=1}^{n}P\left(CM_i\right)}_{\text{Sous l'hypothèse des événements rares}}$$

Hypothèse des événements rares : *Sous l'hypothèse que les événements de base ont une probabilité d'occurrence très faible, la probabilité d'intersection de deux coupes est négligeable devant la somme de leurs probabilités et la probabilité de l'union d'un ensemble de coupes peut être assez bien estimée par la somme des probabilités de ces coupes.*

L'hypothèse des événements rares consiste donc à supposer l'équivalence entre la somme des probabilités des coupes et la probabilité de l'union de ces mêmes coupes.

Un meilleur majorant du risque de référence (un majorant plus petit) est obtenu au moyen de l'algorithme dit de Min Cut Upper Bound (MCUB) [78]. Le principe de cet algorithme est d'approcher le développement de Sylvester-Poincaré en considérant les coupes comme indépendantes [78]. C'est à dire qu'on suppose que :

$$P\left(CM_i\cap CM_j\right)=P\left(CM_i\right)\cdot P\left(CM_j\right)\ \forall i\,\forall j$$

Le développement de Sylvester Poincaré est alors approximé par :

$$\begin{aligned} P\left(\bigcup_{i=1}^{n}CM_i\right) &= \sum_{i=1}^{n}P\left(CM_i\right)-\sum_{i\neq j}P\left(CM_i\right)\cdot P\left(CM_j\right)+\cdots+(-1)^{n-1}\cdot\prod_{i=1}^{n}P\left(CM_i\right)\\ &= 1-\prod_{i=1}^{n}\left(1-P\left(CM_i\right)\right)\end{aligned}$$

De manière équivalente, si on garde l'hypothèse simplificatrice d'indépendance des coupes, on peut comprendre l'algorithme MCUB comme :

$$P\left(\bigcup_{i}^{n}CM_i\right)=1-P\left(\overline{\bigcup_{i}^{n}CM_i}\right)=1-P\left(\bigcap_{i}^{n}\overline{CM_i}\right)\underset{\text{hypothèse indep.coupes}}{\approx}1-\prod_{i=1}^{n}\left(1-P\left(CM_i\right)\right)$$

Algorithme de quantification alternatif

Si l'on veut s'affranchir de l'approximation de Sylvester-Poincaré à l'ordre 1, on peut utiliser l'un des nombreux algorithmes de disjonction des coupes. Ils permettent de disjoindre les coupes de manière efficace, en évitant l'explosion combinatoire. On peut par exemple citer [21], [58] ou encore [76]. Une fois les coupes disjointes, la probabilité de leur intersection est nulle. La probabilité exacte de leur union correspond donc à la somme de leurs probabilités.

Une modélisation au moyen de Diagrammes de Décision Binaires (BDD) permet aussi de calculer la valeur exacte du risque. Cette modélisation alternative est abordée au paragraphe 1.4 du chapitre 1.

Problème lors de la quantification : taille de la fonction de structure

Du fait de leur taille, les modèles EPS ne permettent pas d'avoir l'expression exacte de la fonction de structure. En effet, avec les modèles EPS mis en œuvre à EDF, l'événement CI serait exprimé, de manière non simplifiée, comme l'union d'au moins plusieurs centaines de millions de coupes minimales. Lors de la construction du jeu de coupes, il faudra supprimer (c'est-à-dire ne pas garder en mémoire) les coupes non-significatives avant de pouvoir quantifier la probabilité d'occurrence de l'événement CI à partir de ce jeu de coupes.

Les processus de réduction du jeu de coupes mis en œuvre à EDF sont présentés plus en détail dans la section suivante.

1.2.5 Troncation du jeu de coupes

Les modèles EPS sont de très gros modèles. On ne peut donc pas, avec les limites de mémoire et de capacités de stockage des ordinateurs actuels, générer toutes les coupes correspondant à l'événement CI. Il faut décider d'un critère de sélection des coupes qui seront gardées et de celles qui seront supprimées.

Il existe deux grandes méthodes de troncation d'un jeu de coupes [78] selon que le critère de sélection utilisé est basé sur :
- son ordre, c'est-à-dire sur le nombre d'EB qu'elle contient,
- sa probabilité d'occurrence.

Toutefois, certaines méthodes, telles que celle proposée par Modarres [67], combinent ces deux critères.

Troncation par ordre

Lors de la troncation d'un jeu de coupes, l'objectif est de décider, pour chaque nouvelle coupe générée, si elle doit être conservée ou non dans le jeu de coupes final. La suppression d'une coupe suivant son ordre se fait de la manière suivante : l'utilisateur fixe un nombre maximum d'EB par coupe qu'on appellera S_N (avec S_N un entier positif). Si une coupe contient plus de S_N EB (autrement dit, si son ordre est supérieur à S_N), elle n'est pas gardée en mémoire. Si elle contient au maximum S_N EB (en d'autres termes, si son ordre est inférieur ou égal à S_N), elle est conservée. On obtient alors un jeu de coupes tronqué qui ne contient que des coupes contenant au maximum S_N événements de base, c'est-à-dire des coupes d'ordre inférieur ou égal à S_N.

La troncation basée sur l'ordre des coupes est surtout adaptée aux modèles logiques pour lesquels on ne connaît pas la probabilité d'occurrence des événements de base. Puisqu'on doit tronquer le jeu de coupes, le seul critère disponible est le nombre d'événements par coupe. Si tous les événements de base ont la même probabilité (ce qui est très rarement le cas), ce processus de troncation est équivalent à un processus de troncation probabiliste.

Troncation probabiliste (simple)

La famille de processus de troncation présentée dans ce paragraphe est appelée, dans cette thèse, “processus de troncation simple”, par opposition au processus de troncation double présenté dans le chapitre 2.

Au sein de cette famille, il existe différentes formes de processus de troncation fondées sur la probabilité d'occurrence des coupes. Leur principe de base est le suivant : un seuil de probabilité S_p est fixé. Toutes les coupes dont la probabilité d'occurrence est supérieure à S_p sont conservées, les autres sont supprimées.

Le jeu de coupes tronqué en résultant ne contient que des coupes dont la probabilité d'occurrence est supérieure à S_p. En général, les logiciels supports des EPS fournissent un majorant de la probabilité Δ_{TR} des coupes supprimées (TR pour Troncation du Risque de référence). On appellera par la suite ce majorant Δ_{TRM} (M pour majorant). Pour avoir plus de précisions sur ce point, on peut se référer à [67], à partir duquel ont été développés de nombreux logiciels du commerce, et à [62] pour avoir un aperçu plus récent.

Ce type de troncation est particulièrement bien adapté au calcul du risque de référence car, quelle que soit la valeur de S_p, on gardera toujours les coupes qui contribuent le plus au risque de référence. En effet, puisque le risque est souvent approché en faisant la somme de la probabilité de chaque coupe (approximation de Poincaré[2]) à l'ordre 1, il faut en priorité garder les coupes les plus probables de cette somme pour ne pas trop la sous-estimer.

Choix de la valeur du seuil de troncature probabiliste : La sous-estimation du risque résultant de la troncation du jeu de coupes est un problème bien connu et souvent abordé. On peut par exemple citer l'American Society of Mechanical Engineering (ASME) qui, dans un rapport proposant des approches standardisées pour les EPS [48], spécifie que : “ *la valeur du seuil de troncation doit être obtenue suite à une démarche itérative de telle sorte que l'on puisse démontrer que le risque de référence converge vers la valeur obtenue et qu'aucune séquence accidentelle notable n'a été négligée* ”. De même, l'autorité de sûreté américaine précise bien dans le NUREG-1560 [83] que : “ *les séquences avec une fréquence d'occurrence très faible peuvent être tronquées mais le processus de troncation garantit qu'aucune séquence contribuant significativement au risque n'est supprimée. Ainsi, après la troncation du jeu de coupes, les coupes conservées doivent représenter au moins 95% du risque. De plus, la diminution du seuil de troncature ne doit pas entraîner d'augmentation significative du risque (dans tous les cas, moins de 5%).* ”

C'est en regardant l'évolution du risque en fonction du seuil de troncature que la valeur de S_p a été fixée à 10^{-12} pour les modèles EPS d'EDF. Ainsi, la note “*Guide de réalisation des études de séquences pour les EPS de référence*” [52] précise que : “ *Pour les futures EPS de référence, les seuils suivants ont été retenus* [comme étant un bon] *compromis entre durée de calcul et précision :*
- *Seuils de troncature d'arbres de défaillances : absolu de* 10^{-12} *et relatif de* 10^{-7} *;*
- *Seuil d'élimination de séquences :* 10^{-12}.
Toutefois, si le majorant de l'erreur de calcul, appelé “cutoff error”, est supérieur à 10% du résultat trouvé, on vérifiera que le résultat ne varie pas de façon significative en abaissant le seuil de troncature jusqu'à la diminution de ce majorant en dessous de 10%. Dans le cas où le résultat ne varie pas, les seuils préconisés ci-dessus pourront être conservés. ” La mise au point d'une méthode accélérée de quantification du risque à l'aide de RSW [9] a même permis de trouver un compromis précision/temps de calcul pour un seuil probabiliste S_p de 10^{-14}.

[2]approximation acceptable si l'hypothèse des événements rares est validée, voir §1.2.4 du chapitre 1

1.3 Le fonctionnement de RSW

A EDF, l'outil support des EPS est Risk Spectrum®. Ce logiciel fonctionnant sous Windows (d'où le nom de RSW) est fourni par l'entreprise suédoise RELCON[3]. Il permet, à partir des arbres d'événements associés à chaque initiateur et des arbres de défaillances associés à chaque mission, de produire le jeu de coupes de référence (en général tronqué), et, à partir de ces coupes, de donner une estimation du risque. Les sections suivantes présentent les principes de fonctionnement sur lesquels il repose.

1.3.1 Générer les coupes avec RSW

La construction de la fonction de structure faite par RSW ne se déroule pas telle qu'elle est décrite dans la section 1.2.3 du chapitre 1. En effet, pour éviter une explosion combinatoire, RSW ne prend pas totalement en compte la logique négative lorsqu'il construit la fonction de structure d'une séquence. Il met en œuvre les deux algorithmes présentés ci-dessous.

Algorithme 1

Le premier, appelé "`Ignore Event Tree Success`", qu'on désignera par la suite comme "algorithme 1", génère les coupes d'une séquence en ne prenant pas en compte la porte NON OU qui regroupe les arbres de défaillances modélisant l'échec des missions dont on sait qu'elles sont en succès dans la séquence (cf. [78]). Les coupes exprimant l'occurrence d'une séquence sont donc obtenues avec l'algorithme 1 à partir de l'intersection des jeux de coupes correspondant aux arbres de défaillances des missions considérées en échec dans la séquence. L'algorithme 1 opère donc les simplifications suivantes :

$$\phi_{seq\ j}\left(\underline{e}\right) \underset{algo.\ 1}{\approx} \left(\prod_{\substack{\text{mission } i \text{ en} \\ \text{échec dans} \\ \text{la séquence } j}} \phi_{mission\ i}\left(\underline{e}\right) \right) \underset{\substack{\text{Hypothèse} \\ \text{de cohérence}}}{\longrightarrow} E_{seq\ j} \underset{algo.\ 1}{\approx} \bigcap_{\substack{\text{mission } i \text{ en} \\ \text{échec dans} \\ \text{la séquence } j}} \left(\bigcup_{CM_k \in\ mission_i} CM_k \right)$$

avec $E_{seq\ j}$ l'événement "occurrence de la séquence j".

Exemple : En appliquant l'algorithme 1 à l'exemple de la figure 1.3, on obtient l'arbre de la figure 1.5. A partir de cet exemple, on voit clairement que seules les missions en échec dans la séquence 3 sont prises en compte.

Algorithme 2

Le second algorithme, appelé "`Logical Event Tree Success`", qu'on désignera par la suite comme "algorithme 2", génère d'abord, pour une séquence j donnée, les mêmes coupes que l'algorithme 1. Il supprime ensuite celles d'entre elles qui ne peuvent pas appartenir à la séquence j car leur occurrence implique l'échec d'une ou de plusieurs missions qui sont considérées en succès dans la séquence j.

Exprimé plus formellement, cet algorithme génère les coupes d'une séquence i en trois temps. Tout d'abord, il génère les mêmes coupes que l'algorithme 1. On les appellera $CM_{echec\ seq_i}$. Ensuite, il génère toutes les coupes correspondant à l'échec d'au moins une mission en succès dans la séquence. On les appellera $CM_{succes\ mission}$. Enfin, il supprime parmi toutes les coupes générées à la première étape celles qui contiennent au moins une des coupes générées à la seconde étape. C'est à dire que la coupe j, notée $CM_{echec\ seq_i,j}$, sera supprimée si :

$$\exists\, CM_{succes\ mission_k} \quad \text{telle que} \quad CM_{succes\ mission_k} \subset CM_{echec\ seq_i,j}$$

Ce processus de suppression des coupes, générées par l'agorithme 1 et contenant une coupe correspondant à une mission en succès est appelé processus de "`Delete Term`". L'algorithme 2 opère donc les simplifications suivantes :

[3] Voir les sites `http ://www.riskspectrum.com` et `http ://www.relcon.se`

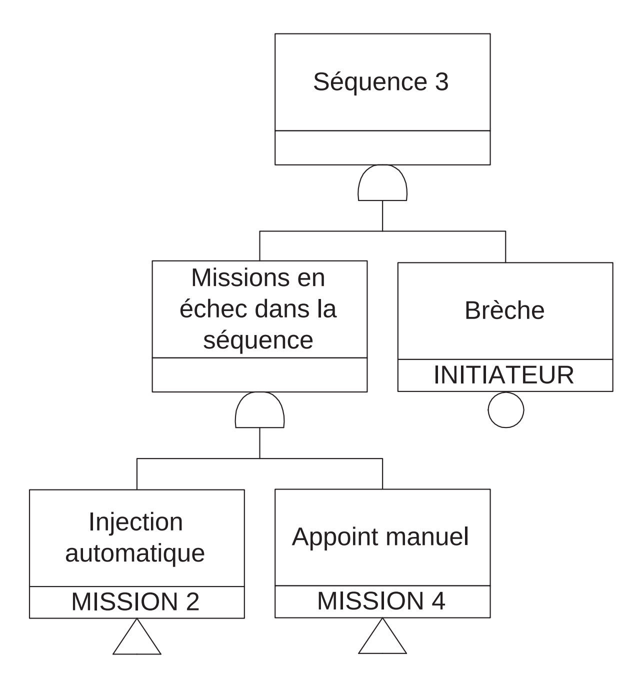


FIG. 1.5 – *Arbre de défaillances généré par RSW avec l'algorithme 1, pour modéliser la séquence 3 de l'arbre de la figure 1.1*

$$E_{seq\ j} \underset{algo.\ 1}{\approx} \bigcap_{\substack{\text{mission } i \text{ en} \\ \text{échec dans} \\ \text{la séquence } j}} \left(\bigcup_{\substack{CM_l \in\ mission_i\ , \\ \nexists\, CM_{succes\ mission_k} \\ \text{telle que} \\ CM_{succes\ mission_k} \in CM_l}} CM_l \right)$$

Exemple : On prend l'exemple de la séquence 6 de l'arbre d'événements de la figure 1.1 page 10. On simplifie chaque mission en supposant que l'occurrence de la mission 1 (Détection auto. de la brèche) correspond à deux coupes : $(EB_{capteur}) \cup (EB_{elect.})$, que la mission 2 (Injection auto. ou manu. de réfrigérant) correspond aux coupes : $(EB_{pompe}) \cup (EB_{elect.})$ et que la mission 3 (détection par les opérateurs) correspond à un seul événement de base : EB_{Op}. L'initiateur est modélisé au moyen d'un seul EB : $EB_{brèche}$.

Sous ces hypothèses, l'algorithme 1 génère deux coupes qui correspondent à la séquence 6 : $(EB_{brèche} \cap EB_{elect.} \cap EB_{Op}) \cup (EB_{brèche} \cap EB_{capteur} \cap EB_{Op})$ L'algorithme 2 se déroule en trois étapes. Il génère d'abord les mêmes coupes que l'algorithme 1. Nous les connaissons déjà. Ensuite il génère les coupes correspondant à l'échec des missions considérées en succès dans la séquence étudiée. Dans la séquence 6, seule la mission 2 est en succès. Les coupes correspondant à son échec sont : $(EB_{pompe}) \cup (EB_{elect.})$. Enfin il supprime parmi les coupes correspondant à l'algorithme 1 celles qui contiennent l'échec de la mission 2. La coupe $(EB_{brèche} \cap EB_{elect.} \cap EB_{Op})$ contient la coupe $(EB_{elect.})$ de la mission 2. Cette coupe ne peut pas s'être produite sinon la séquence 9 serait réalisée. L'algorithme 2 supprime donc cette coupe et le jeu de coupes correspondant à la séquence 6 généré par l'algorithme 2 est finalement : $(EB_{brèche} \cap EB_{capteur} \cap EB_{Op})$

Probabilité d'occurrence de l'événement CI en fonction de l'algorithme

Quel que soit l'algorithme (1 ou 2) utilisé, RSW produit toujours un jeu de coupes pour chaque séquence. Les coupes correspondant à l'événement CI sont alors obtenues en fusionnant les jeux de coupes de chaque séquence conduisant aux conséquences inacceptables (événement CI). Quel que soit l'algorithme, on retrouve donc bien que :

$$CI = \bigcup_j E_{seq\ j}$$

avec $E_{seq\ j}$ calculé de manière différente suivant l'algorithme utilisé.

Suivant l'algorithme utilisé, on peut montrer que le risque estimé est plus ou moins élevé. En effet, quelle que soit la séquence considérée, on a :

$$E_{seq\ j}|_{algo\ 2} \subseteq E_{seq\ j}|_{algo\ 1}$$

avec :

$E_{seq\ j}|_{algo\ 1}$ l'événement "occurrence de la séquence j" exprimé au moyen des coupes issues de l'algorithme 1,

$E_{seq\ j}|_{algo\ 2}$ l'événement "occurrence de la séquence j" exprimé au moyen des coupes issues de l'algorithme 2,

En effet, avec l'algorithme 2, l'événement "occurrence de la séquence j" est exprimé à partir d'un jeu de coupes issu de celui généré par l'algorithme 1 correspondant à ce même événement dont certaines coupes ont pu être enlevées. Finalement, on trouve que :

$$CI|_{algo\ 2} \subseteq CI|_{algo\ 1}$$

avec :

$CI|_{algo\ 1}$ "l'événement occurrence des circonstances inacceptables" exprimé au moyen des coupes issues de l'algorithme 1,

$CI|_{algo\ 2}$ l'événement "occurrence des circonstances inacceptables" exprimé au moyen des coupes issues de l'algorithme 2,

car

$$CI|_{algo\ 2} = \bigcup_j E_{seq\ j}|_{algo\ 2} \quad \text{et} \quad CI|_{algo\ 1} = \bigcup_j E_{seq\ j}|_{algo\ 1} \quad \text{et} \quad E_{seq\ j}|_{algo\ 2} \subseteq E_{seq\ j}|_{algo\ 1} \forall j.$$

Enfin, on peut retenir que ces deux algorithmes, si les jeux de coupes qu'ils produisent ne sont pas tronqués, font une estimation du risque de référence pessimiste ou exacte. C'est à dire [78] que l'on a :

$$P\left(CI|_{algo\ 1}\right) \geq P\left(CI|_{algo\ 2}\right) \geq P\left(CI\right)$$

1.3.2 Outils de troncation proposés par RSW

RSW propose à la fois une troncation du jeu de coupes par ordre identique à celle présentée dans la section 1.2.5 du chapitre 1 et plusieurs processus de troncation probabilistes [78].

La troncation probabiliste simple repose sur trois critères différents utilisés de manière conjointe :

1. Un seuil absolu, qu'on appellera $S_{p,A}$ et qui est un réel appartenant à l'intervalle $[0; 0,999]$: si ce seuil était utilisé seul, toutes les coupes dont la probabilité est supérieure à $S_{p,A}$ seraient conservées.
2. Un seuil relatif, qu'on appellera $S_{p,r}$ et qui est un réel appartenant à l'intervalle $[0; 0,999]$: si ce seuil relatif était utilisé seul, la valeur du seuil de troncature probabiliste S_p dépendrait de la valeur qu'on a fixée pour $S_{p,r}$ et de la valeur du risque de référence estimée à partir d'un développement de Poincaré à l'ordre 1. Le principe de la troncation du jeu de coupes avec un seuil relatif est le suivant :

- l'utilisateur fixe la valeur de $S_{p,r}$.
- Le risque est approximé par la somme des probabilités de toutes les coupes minimales qu'on appellera $QSUM$.
- Un seuil de troncature probabiliste S_p est calculé comme $QSUM_i \cdot S_{p,r}$

Si un seuil relatif était utilisé seul, on garderait toutes les coupes dont la probabilité est supérieure ou égale à $P(CI) \cdot S_{p,r}$. Cependant, ce critère ne peut être utilisé seul pour une EPS car il nécessite de générer toutes les coupes.

3. Un seuil sur le nombre de coupes générées, qu'on appellera $S_{p,N}$ et qui est un entier positif compris entre 1 et 10 millions. Si ce seuil est utilisé seul (c'est le cas quand $S_{p,A} = 0$ et $S_{p,r} = 0$), on gardera les $S_{p,N}$ coupes les plus probables avec $S_{p,N}$ fixé par l'utilisateur.

   Dans la mesure où $S_{p,N}$ ne peut valoir plus de dix millions, on ne pourra jamais, avec la version actuelle de RSW, générer un jeu de plus de 10 millions de coupes.

Ces trois seuils sont toujours utilisés conjointement, donc le seuil probabiliste S_p effectivement mis en œuvre sera tel que :

$$S_p = max\left(S_{p,A}\ ;\ P(CI) \cdot S_{p,r}\ ;\ P\left(CM_{S_{p,N}}\right)\right)$$

avec

$P\left(CM_{S_{p,N}}\right)$ la probabilité de la ${S_{p,N}}^{eme}$ coupe lorsque les coupes sont classées par ordre décroissant.

$P(CI)$ la probabilité estimée du risque

Quel que soit le processus de troncation probabiliste (simple) utilisé , RSW fournit un majorant de la probabilité des coupes tronquées (Δ_{TRM}). On sait donc que quel que soit le processus de troncation et quel que soit le seuil choisi : $R \leq R_{estimé} + \Delta_{TRM}$

1.3.3 Prise en compte des événements dépendants

Principe de la modélisation des défaillances de causes communes dans les EPS d'EDF

L'hypothèse d'indépendance des EB n'est qu'une hypothèse simplificatrice, qui peut parfois être inadaptée. Dans certains cas, des défaillances de causes communes (DCC) sont introduites dans les modèles pour pouvoir localement abandonner cette hypothèse. La norme NF X60-500 définit les défaillances de causes communes comme "*des défaillances affectant ou pouvant affecter simultanément ou en cascade, à partir d'une même cause, tout ou partie des composants d'une entité ou éventuellement plusieurs entités à la fois*". Le but est de modéliser le fait qu'une même cause peut affecter simultanément plusieurs matériels, en particulier les matériels redondants. En termes d'événements, la modélisation des DCC revient à considérer que plusieurs EB peuvent être réalisés en même temps par une même cause.

Plusieurs modèles paramétriques ont été proposés. On peut citer entre autres [78], [69] et [26]. Le choix de modélisation des DCC fait pour les EPS d'EDF dans RSW est la modélisation des Lettres Grecques Multiples (MGL). Ainsi, pour chaque groupe DCC de taille inférieure ou égale à quatre (cf. [8]), on définit les paramètres β, γ et δ par :

β la probabilité de défaillance par mode commun d'au moins deux composants du groupe DCC, sachant qu'un composant spécifique est déjà défaillant.

γ la probabilité de défaillance par mode commun d'au moins trois composants du groupe DCC, sachant que deux, dont un spécifique, sont déjà défaillants.

δ la probabilité de défaillance par mode commun d'au moins quatre composants du groupe DCC, sachant que trois, dont un spécifique, sont déjà défaillants.

On peut alors définir Q_i comme la probabilité de défaillance de i composant spécifiques parmi m du fait de la même cause :

$$Q_1 = (1-\beta)\cdot Q_{tot} \quad ; \quad Q_2 = \frac{\beta\cdot(1-\gamma)\cdot Q_{tot}}{m-1} \quad ; \quad Q_3 = \frac{\beta\cdot\gamma\cdot(1-\delta)\cdot Q_{tot}}{m-1} \quad ;$$
$$Q_4 = \beta\cdot\gamma\cdot\delta\cdot Q_{tot}$$

$$\text{avec } k_2 = \begin{cases} m-1 \text{ si } m>2 \\ 1 \text{ sinon} \end{cases} \quad \text{et} \quad k_3 = \begin{cases} m-1 \text{ si } m>3 \\ 1 \text{ sinon} \end{cases}$$

Avec
m la taille du groupe DCC.
Q_{tot} la probabilité de défaillance totale d'un composant du groupe (défaillance intrinsèque ou défaillance de causes communes)

Les paramètres β, γ, δ et Q_{tot} peuvent être estimés à partir de l'analyse du retour d'expérience [26].

Si le groupe DCC ne contient que trois événements de base ($m = 3$), alors $\delta = 0$. De même, si $m = 2$, alors $\gamma = \delta = 0$. En effet, si on prend l'exemple d'un groupe DCC ne contenant que trois EB, la probabilité dé défaillance par mode commun d'au moins quatre composants est nulle. On a donc bien $\delta = 0$ et donc $Q_4 = 0$.

Mise en œuvre de ce modèle dans RSW

La quantification des coupes par RSW nécessite que les événements de base soient considérés comme indépendants. En effet, son fonctionnement nécessite entre autres qu'un EB_i ait toujours la même probabilité (quel que soit l'état des autres EB et quel que soit le contexte). Pour pouvoir modéliser des EB appartenant à des groupes DCC, RSW décompose l'événement "occurrence de l'EB_i" en autant d'événements qu'il y a de cas possibles. On appellera ces événements des EB_{DCC}. Ainsi, pour un groupe DCC contenant au moins quatre EB, on considérera séparément :

- la défaillance intrinsèque de EB_i (notée $EB_{int,i}$),
- la défaillance de EB_i et de EB_j suite à une cause commune pour chaque valeur de j différente de i (noté $EB_{DCC;i,j}$),
- la défaillance de EB_i, de EB_j et de EB_k suite à une cause commune pour chaque valeur de j et de k différente de i (notée $EB_{DCC;i,j,k}$),
- la défaillance simultanée de tous les EB du groupe DCC pour une même cause commune (notée $EB_{DCC;ALL}$).

De ce fait, l'occurrence de EB_i appartenant à un groupe DCC est alors modélisée par RSW au moyen d'un arbre de défaillances (cf. figure 1.6) regroupant sous une porte OU un EB modélisant la défaillance de i pour des causes intrinsèques (notée $EB_{int,i}$), ainsi que des EB indépendants modélisant les défaillances de causes communes possibles impliquant cet EB_i (les EB_{DCC}).

Bien que cette propriété ne soit pas prise en compte dans la modélisation des DCC faite par RSW (cf. figure 1.6), deux EB d'un groupe DCC sont mutuellement exclusifs [28]. Ainsi, $EB_{DCC;i,j} \cap EB_{DCC;i,k} = \emptyset$ si $j \neq k$. De même, $EB_{DCC;j,k} \cap EB_{int,i} = \emptyset$, $\forall j$.

Il est à noter que RSW ne considère que les défaillances de deux, trois ou tous les EB suite à une cause commune. Il ne considérera, par exemple, pas la défaillance de cinq composants parmi huit [78]. Si EB_i appartient à un groupe DCC d'ordre supérieur ou égal à quatre, RSW exprimera donc cet événement de base comme :

$$EB_i = EB_{int,i} \cup \left(\bigcup_{i\neq j} EB_{DCC;i,j} \right) \cup \left(\bigcup_{i\neq j, i\neq k, j\neq k} EB_{DCC;i,j,k} \right) \cup EB_{DCC;tous}$$

Exemple : Supposons que les EB 1, 2 et 3 appartiennent à un groupe DCC d'ordre 3. Supposons qu'il modélisent les défaillances des pompes 1, 2 et 3. Dans ce cas, la figure 1.6 représente la modélisation de la défaillance de la pompe 1 mise en œuvre par RSW. On voit

donc que pour modéliser la défaillance de la pompe 1, RSW considère l'occurrence de l'une ou l'autre des défaillances de cause commune pouvant l'affecter ainsi que sa défaillance intrinsèque.

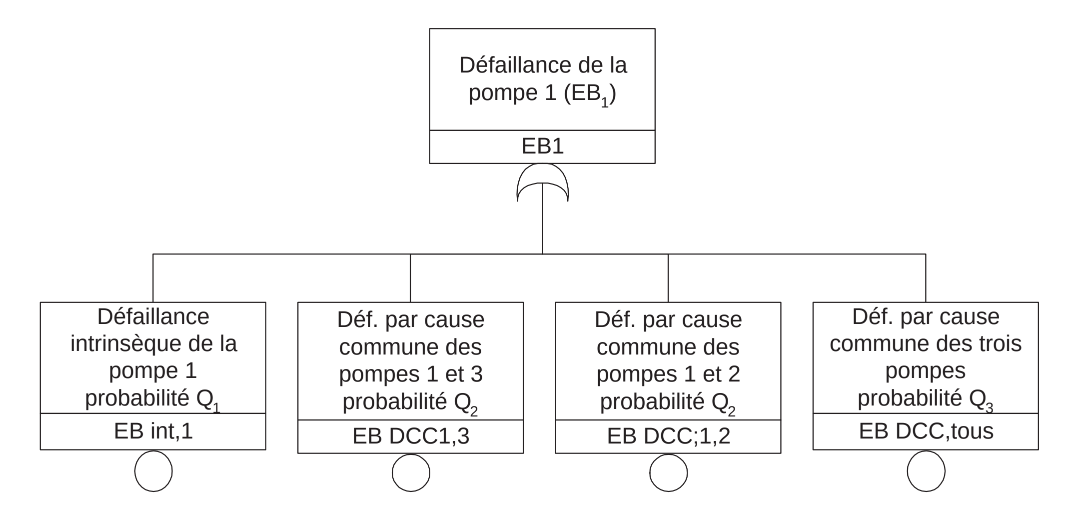


FIG. 1.6 – *Arbre de défaillances modélisant la défaillance de l'EB1*

La probabilité de $EB_{int,1}$ est de $Q_1 = (1 - \beta) \cdot Q_{tot}$. La probabilité de $EB_{DCC\ 1,3}$ et de $EB_{DCC\ 1,2}$ est de $Q_2 = \dfrac{\beta \cdot (1-\gamma) \cdot Q_{tot}}{2}$ et enfin la probabilité de $EB_{DCC,tous}$ est de $Q_3 = \beta \cdot \gamma \cdot Q_{tot}$.

1.4 Comparaison des EPS d'EDF avec les autres types de modélisation

Dans cette section, la modélisation des EPS mise en œuvre à EDF (et par la plupart des autres exploitants à travers le monde), telle qu'elle est décrite dans la section 1.2 de ce chapitre, sera comparée aux autres types de modélisation pouvant permettre de calculer le risque de référence.

1.4.1 La modélisation par Diagramme de Décision Binaire (BDD)

Principe de la modélisation par BDD

Un BDD est une représentation graphique (un graphe acyclique ordonné) d'une fonction booléenne qui permet de représenter de manière condensée l'ensemble des états du vecteur d'état $\underline{e}$ et la valeur de la fonction de structure (zéro ou un) qui y est associée [75]. Appliquée à la modélisation de la fonction de structure Φ qui exprime l'occurrence ou la non-occurrence de l'événement CI, sa modélisation au moyen d'un BDD permet d'obtenir un ensemble d'événements, tous disjoints, dont l'union correspond à l'événement CI.

La représentation d'une fonction de structure sous la forme du diagramme de décision binaire (BDD) repose sur l'application récursive de la décomposition de Shannon[4] à la fonction de structure $\Phi(\underline{e})$ [75], [74].

Décomposition de Shannon : *La décomposition de Shannon d'une fonction de structure $\Phi(\underline{e})$ pour la variable d'état e_i s'opère en exprimant Φ comme :*

$$\Phi(\underline{e}) = e_i \cdot \underbrace{\Phi(\underline{e}_{-i}, e_i = 1)}_{\text{noté } \Phi_{1_i}(\underline{e})} + (1 - e_i) \cdot \underbrace{\Phi(\underline{e}_{-i}, e_i = 0)}_{\text{noté } \Phi_{0_i}(\underline{e})}$$

[4]aussi appelée décomposition pivotale

Avec :

$\underline{e}_{-i}$	*le vecteur d'état de tous les événements excepté l'événement i*
$\Phi_{1_i}\left(\underline{e}_{-i}, e_i = 1\right)$	*la fonction de structure quand l'événement i est réalisé.*

La décomposition récursive d'une fonction de structure se fait, tout d'abord, en ordonnant les variables[5]. On décompose alors la fonction de structure suivant la première de ces variables comme dans l'encadré ci-dessus. Ensuite, on décompose les deux sous-fonctions de structures obtenues ($\Phi_{1_i}(\underline{e})$ et $\Phi_{0_i}(\underline{e})$) au moyen d'une décomposition de Shannon suivant la deuxième variable, et ainsi de suite.

On obtient alors une expression de la fonction de structure comme une somme de sous-fonctions correspondant aux différentes combinaisons possibles des événements de base. On peut la représenter de manière graphique au moyen d'un arbre de Shannon. Cette représentation très volumineuse est condensée au moyen des deux règles suivantes (règles de Shannon) :
- deux nœuds ayant les mêmes nœuds fils peuvent être fusionnés,
- un nœud ayant deux nœuds fils identiques peut être supprimé.

Suite à cette simplification, on obtient une liste d'impliquants premiers qui sont des intersections d'événements et de "non-événements" correspondant à l'événement CI. A la différence des coupes, les impliquants contiennent la non-occurrence de certains EB. C'est à dire qu'ils peuvent contenir l'événement "non-occurrence de l'événement de base i " ($\overline{EB_i}$), par exemple.

Les impliquants sont des événements tous disjoints deux à deux. La quantification exacte de la probabilité d'occurrence de l'événement CI au moyen d'un BDD peut donc se faire en faisant la somme des probabilités des impliquants. Si on fait l'hypothèse d'indépendance des événements de base, alors la probabilité d'un impliquant quelconque s'exprime comme le produit des probabilités d'occurrence des EB dont l'occurrence est nécessaire à celle de l'impliquant par le produit des probabilités de non-occurrence des EB dont la non-occurrence est nécessaire à l'occurrence de l'impliquant.

Exemple : Supposons qu'on ait l'arbre de défaillances de la figure 1.7 reposant sur les événements de base A, B et C. L'occurrence de l'événement CI, exprimée au moyen de l'arbre de défaillances, est donc :$A \cap B \cup C$.

On fait le choix d'ordonner les variables en considérant l'événement A, puis B, puis C. Suite à la première décomposition pivotale (décomposition de Shannon) on obtient :
$A \cap (B \cup C) \cup \overline{A} \cap (C)$
Après la seconde décomposition pivotale, on obtient :
$A \cap \left(B \cap (VRAI) \cup \overline{B} \cap (C)\right) \cup \overline{A} \cap \left(B \cap (C) \cup \overline{B} \cap (C)\right)$
Enfin, après la dernière décomposition pivotale, on obtient :
$A \cap \left(B \cap \left(C \cup \overline{C}\right) \cup \overline{B} \cap (C)\right) \cup \overline{A} \cap \left(B \cap (C) \cup \overline{B} \cap (C)\right)$
$= (A \cap B \cap C) \cup \left(A \cap B \cap \overline{C}\right) \cup \left(A \cap \overline{B} \cap C\right) \cup \left(\overline{A} \cap B \cap C\right) \cup \left(\overline{A} \cap \overline{B} \cap C\right)$
La figure 1.8 page 25 présente l'arbre de Shannon correspondant à notre exemple et le BDD qui en découle après sa simplification.

Les impliquants qui résultent de cette simplification sont :

$$(A \cap B) \cup \left(A \cap \overline{B} \cap C\right) \cup \left(\overline{A} \cap C\right)$$

Avantages de cette modélisation

La modélisation par BDD part de la fonction de structure complète, considère toutes les combinaisons possibles (arbre de Shannon) et condense cette information (règles de Shannon)

[5] Le choix de cet ordre conditionnera la taille du BDD généré. Différentes heuristiques d'ordonnancement existent. Pour en avoir un aperçu, voir [17]

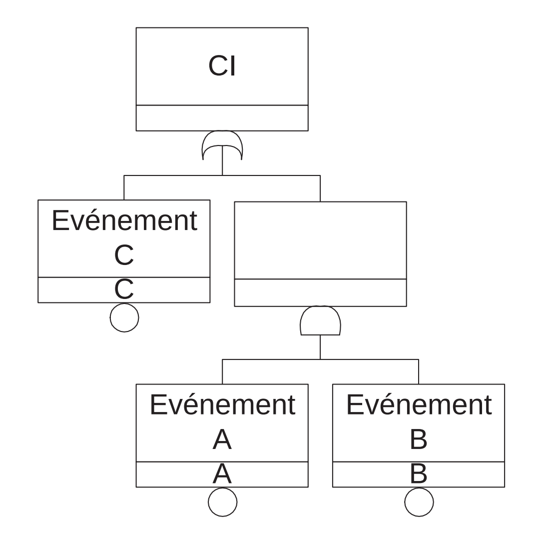


FIG. 1.7 – *Arbre de défaillances de l'exemple*

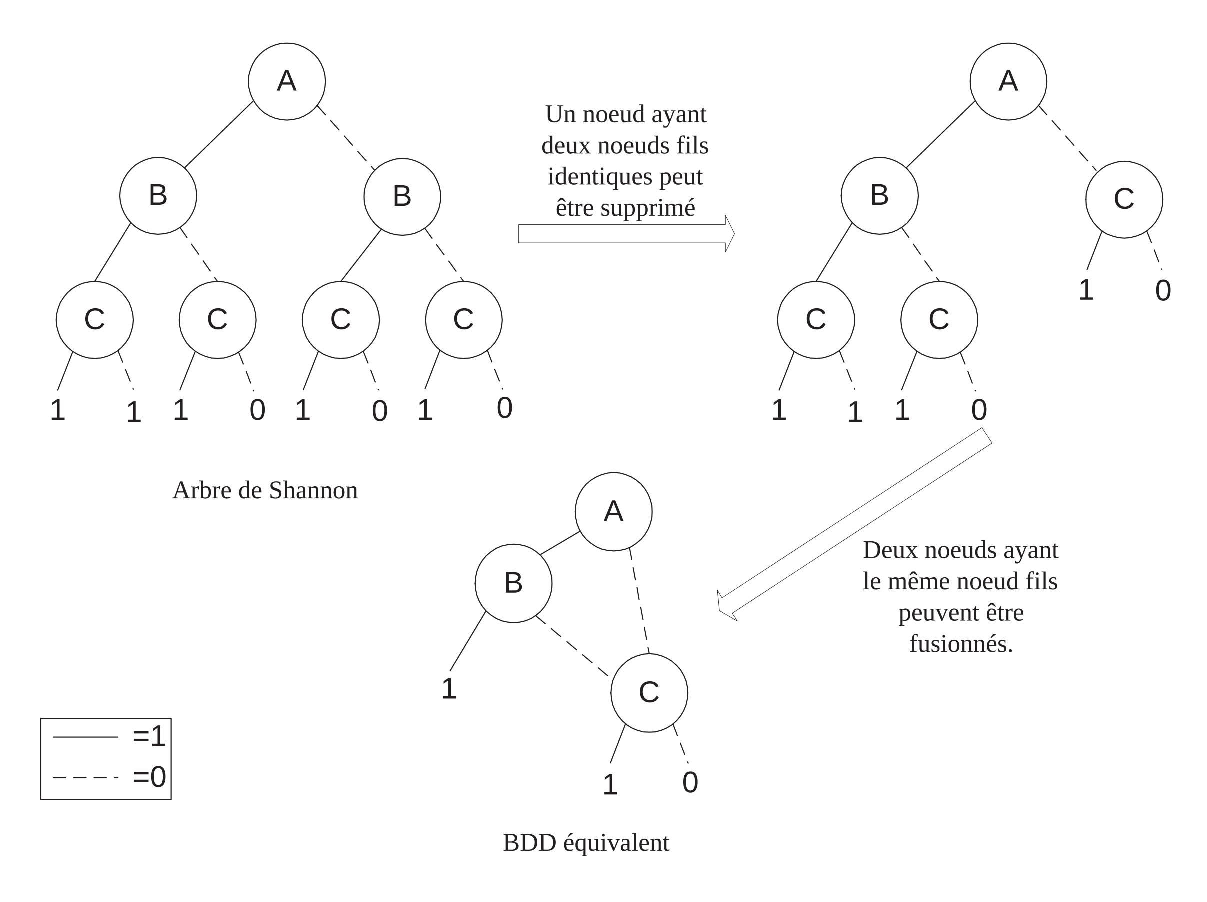


FIG. 1.8 – *Arbre de Shannon et BDD équivalent à l'arbre de défaillances de la figure 1.7*

sans en modifier le sens. On n'a donc pas besoin de l'hypothèse de cohérence de la fonction de structure comme dans le cas d'une expression de la fonction de structure au moyen de coupes [10]. Contrairement à une modélisation sous forme de coupes minimales, on peut très bien modéliser le comportement de systèmes non-cohérents où l'occurrence d'un événement i est nécessaire à l'occurrence de l'événement CI dans certains contextes et sa non-occurrence est nécessaire à l'occurrence de ce même événement CI dans d'autres contextes. La modélisation

de la fonction de structure au moyen d'un BDD permet donc la prise en compte des événements en succès, contrairement à la modélisation actuelle des EPS d'EDF.

De plus, comme on l'a vu précédemment, sous réserve que les événements de base soient indépendants, on peut quantifier au moyen d'un BDD le risque exact, sans avoir recours à une approximation telle que l'approximation de Poincaré à l'ordre un. Avec une modélisation de type BDD, l'expression exacte de la probabilité d'occurrence de l'événement CI est obtenue au moyen d'une simple somme des probabilités d'occurrence de chaque impliquant.

Enfin, sur le plan des outils supports, bien qu'une troncation de la fonction de structure soit toujours possible dans le cadre d'une modélisation au moyen d'un BDD (cf. [22]), les outils supports des BDD tels que Aralia® [6] proposent souvent une expression exacte de la fonction de structure (pas de troncation). Pour une même fonction de structure, il existe des cas (cf. [16]) où un codage sous forme de BDD sans troncation est possible avec Aralia alors qu'il ne l'est pas avec RSW (on dépasse la limite de 10 millions de coupes). Aralia permet donc, au moins dans certains cas, un meilleur stockage de l'information. On peut alors, pour certaines fonctions de structure, ne pas les tronquer alors que RSW y serait contraint. Le résultat en est d'autant plus précis.

Pour plus d'informations sur les avantages des BDD sur une méthode de quantification classique basée sur les coupes, on peut citer [36, 37, 44, 45, 46].

Application de cette modélisation aux EPS

Si aucune troncation de la fonction de structure n'est opérée, on peut ne pas réussir à modéliser sous forme de BDD les fonctions de structure de très grande taille. C'est le cas pour les EPS, comme le souligne Epstein dans [47], "*la quantification d'une EPS au moyen d'un BDD échoue du fait de l'explosion exponentielle de la mémoire requise*". Si la fonction de structure est simplifiée comme proposé dans [70], on perd l'intérêt d'une résolution exacte.

Dans [46], Epstein étudie la pertinence du niveau de détail d'une EPS. Il apparaît alors que seul un petit nombre d'événements de base contribue réellement à la valeur du risque de référence. Ainsi, dans le modèle utilisé dans cet article, certains EB sont reliés à la porte sommet de l'arbre de défaillances modélisant l'événement CI par 17 portes logiques ET successives. Pourtant, on estime le risque comme valant 98% de sa valeur calculée avec une EPS complète quand on ne considère que les EB situés à, au plus, quatre portes ET de la porte sommet. De cette étude, on déduit que les EPS ont un niveau de détail bien supérieur à celui requis pour avoir une bonne estimation du risque de référence.

On peut donc en conclure qu'une EPS condensée, où tous les événements situés loin (en termes de portes ET) de la porte sommet de l'arbre de défaillances modélisant l'événement CI seraient négligés ou regroupés dans un même EB, produirait une bonne estimation du risque de référence. Cette EPS condensée de beaucoup plus petite taille pourrait très probablement être modélisée au moyen d'un BDD.

Si, dans l'immédiat, les EPS non simplifiées telles que celles développées par EDF ne peuvent être modélisées sans simplification au moyen d'un BDD, Fleming considère dans le NUREG 6813 [49] que "*les BDD, qui permettent de considérer les arbres de défaillances sans simplifier la fonction de structure* [qu'ils expriment]*, peuvent être une solution à long terme* [au problème des incertitudes]".

1.4.2 Modélisation au moyen d'un graphe de Markov

Principe de la modélisation de Markov

La modélisation d'un système physique au moyen d'un processus de Markov repose sur :

[6]Voir le site `http ://arboost.com`

1. l'identification de tous les états du système. Tous les états du système correspondent à toutes les valeurs possibles du vecteur $\underline{e}$. Une fois identifiés, ces états sont répartis en :
   - *état de fonctionnement parfait* (aucune panne) souvent considéré comme étant l'état initial ($\forall i, e_i = 0$),
   - *états dégradés* qui correspondent aux états de marche (états pour lesquels $\exists i \ / \ e_i = 1, \ \Phi(\underline{e}) = 0$),
   - *états de panne.* (Les états de panne sont les états pour lesquels $\Phi(\underline{e}) = 1$.)

   Dès qu'on considère un système comportant plusieurs événements élémentaires, le nombre d'états explose du fait de la combinatoire qui est en 2^n avec n le nombre d'événements élémentaires.

2. la définition des taux de transition entre états permettant la construction de la matrice des taux de transition. Dans la définition de ces taux de transition, il est à noter que, pour pouvoir utiliser un processus Markovien de saut, le système doit être considéré comme étant sans mémoire et que ses taux doivent donc être constants. La loi définissant le temps de séjour dans l'état i est donc une loi exponentielle[7].

Au moyen de l'état initial et de la matrice de transition stochastique, on arrive à obtenir une estimation de la probabilité d'occurrence de l'état de panne en fonction du temps.

La modélisation du comportement d'un système au moyen d'un processus de Markov donne donc sa probabilité d'être de panne en fonction du temps, mais on peut aussi évidemment en déduire la fiabilité ou la disponibilité moyenne sur 24 heures, ainsi que tous les autres indicateurs classiques de la fiabilité (MTTF, MTTR, etc.).

Si on admet, comme c'est le cas dans les EPS, que les taux de transition soient considérés comme constants, cette modélisation est plus riche que celle mise en œuvre actuellement dans les EPS. En effet, elle peut se passer de l'hypothèse d'indépendance des événements de base et elle donne la probabilité instantanée de panne, contrairement aux EPS, qui ne donnent qu'une probabilité moyenne estimée sur 24 heures. Elle permet de bien mieux prendre en compte la dynamique d'un accident en considérant les défaillances successives et les réparations éventuelles. Ainsi, dans le cadre de deux systèmes en redondance passive par exemple, on ne considère pas la probabilité de défaillance du système en secours sur 24 heures mais sur la durée effective de sa sollicitation à partir du moment où le premier système défaille.

Application de cette modélisation aux EPS

Encore plus que pour les BDD, le problème de la taille des modèles est crucial lorsqu'on veut utiliser une modélisation au moyen d'une chaîne de Markov. Sans aucune simplification, on ne peut considérer plus de quelques dizaines de composants. Une EPS de référence en contenant plusieurs milliers, on ne peut donc pas, sans avoir recours à des simplifications, envisager de modéliser une EPS au moyen de graphes de Markov.

Deux types de solutions peuvent être mis en œuvre parallèlement :

- Le système "centrale nucléaire" peut être divisé en sous-systèmes indépendants. Ces sous-systèmes sont modélisés indépendamment et le risque de référence est obtenu par enchaînement numérique à partir de la probabilité de défaillance de chaque sous-système.
- Les différents états peuvent être regroupés pour réduire le graphe et obtenir une matrice de transition stochastique de taille acceptable.

On peut donner deux exemples explicitant ces types d'approche. Pour illustrer la méthode de regroupement d'états, on peut citer la thèse de Derode [25], qui propose une démarche de

[7] En effet, seule la loi exponentielle permet d'avoir :
$\textit{taux transition}_{i,j} = \lim_{\Delta_t \to 0} \left(\frac{P\left(\underline{e}_{t+\Delta_t} = \underline{e}_j / \underline{e}_t = \underline{e}_i\right)}{\Delta_t} \right) = \textit{constante} \ \forall t$ avec $\underline{e}_i$ et $\underline{e}_j$ deux états spécifiques du système et $\underline{e}_t$ l'état du système à l'instant t

réduction du nombre d'états en agglomérant les états dits "rapides" dans lesquels le système ne passe que peu de temps.

Le fractionnement d'un système en sous-systèmes indépendants était lui à la base du logiciel LESSEPS (c.f. [7]) dont le principe de fonctionnement était, de manière schématique, de réunir, au moyen d'arbres d'événements, des graphes de Markov modélisant certains sous systèmes indépendants avec d'autres types de modélisation comme des arbres de défaillances modélisant les autres sous-systèmes. Cette modélisation nécessitait d'expliciter toutes les interdépendances avec des graphes spécifiques. Cette méthode, lourde à mettre en œuvre, a depuis été abandonnée. Cependant, l'existence de ce modèle EPS sous LESSEPS a démontré la faisabilité de l'utilisation de graphes de Markov, mis en œuvre conjointement à d'autres types de modélisations probabilistes et réunis au moyen d'enchaînements numériques.

1.4.3 Modélisation au moyen d'un réseau de Pétri

Principe des réseaux de Pétri

La modélisation par les réseaux de Pétri est une modélisation "événementielle". Ces réseaux décrivent, au moyen d'un formalisme graphique, le fonctionnement d'un système à l'aide de jetons et de transitions (pour plus d'information voir par exemple [56]). Ils permettent de représenter une très grande variété de comportements. On peut ensuite, au moyen d'une simulation de Monte-Carlo, simuler des "histoires" du système et déduire des ces dernières le risque de référence, entre autres.

Application aux EPS

Comme toutes les modélisations basées sur des simulations de Monte Carlo, aucune hypothèse contraignante (indépendance des événements, taux de défaillance constants...) n'est nécessaire mais il faut simuler un très grand nombre d'histoires pour voir apparaître des événements rares. Dans la mesure où les EB des EPS ont, en général, une probabilité d'occurrence faible, le "coût en temps de calcul" qu'aurait une quantification du risque de référence d'une EPS est prohibitif.

Un autre gros point faible des réseaux de Petri est "*leur incapacité à décrire de manière simple des propagations ou des fonctions de structure*" [15]. Ce problème est particulièrement bloquant quand on considère la taille de la fonction de structure modélisée dans une EPS. La modélisation d'une EPS au moyen de réseaux de Petri demanderait donc de complètement repenser la description logique du fonctionnement de l'installation.

2 Les facteurs d'importance

Initialement, les EPS avaient pour but d'estimer le risque de référence et d'identifier les séquences prépondérantes. Leur niveau de détail et la modélisation qui les supporte permettent toutefois de définir des mesures d'importance permettant d'étudier, pour chaque composant ou chaque événement, son importance vis-à-vis du risque. Ces mesures d'importance, appelées aussi facteurs d'importance, sont des outils d'aide à la décision qui donnent aux concepteurs et aux exploitants des centrales nucléaires les moyens d'identifier les pistes d'améliorations possibles, les événements-clefs ou la conduite à tenir face à un événement imprévu.

Cette section présente ces différents facteurs d'importance ainsi que leurs modes de calcul pour des événements de base indépendants, pour des EB appartenant à des groupes DCC et pour des ensembles d'EB.

2.1 Définition des différents facteurs d'importance

Dans cette partie, ne seront présentés que des facteurs d'importance basés sur des composants binaires (marche/panne) employés dans des modèles booléens tels que décrits dans la section 1. Avant de présenter ces facteurs d'importance, nous rappellerons les notations utiles à leur définition, ainsi que quelques définitions nécessaires à leur interprétation.

2.1.1 Rappel des notations

Pour pouvoir définir les différents facteurs d'importance, nous utiliserons les notations suivantes :

EB_i	l'événement élémentaire i aussi appelé événement de base
e_i	la variable booléenne d'état de l'événement EB_i
$\underline{e}$	le vecteur d'état regroupant les variables e_i ($\underline{e} \in [0;1]^n$)
p_i	la probabilité d'occurrence de l'EB_i ($p_i = P(e_i = 1)$)
$\underline{p}$	le vecteur regroupant les probabilités des différents événements de base $\left(\underline{p} \in [0,1]^n\right)$
CI	l'événement "atteinte des Conséquences Inacceptables"
Δ_{TR}	la valeur de la sous-estimation du risque due à la troncation du jeu de coupes. La lettre T rappelle qu'il ne s'agit que de l'impact de la troncation et la lettre R qu'il s'agit de l'impact sur le risque.
Δ_{TRM}	le majorant de la valeur de la sous-estimation du risque due à la troncation du jeu de coupes (M pour majorant)
$\Phi(\underline{e})$	la fonction de structure exprimant à partir du vecteur d'état (réalisé ou non) de chaque événement de base l'occurrence de l'événement "atteinte de conséquences inacceptables"
$\phi(\underline{e})$	la fonction de structure d'un sous-système. Si $\phi(\underline{e}) = 1$, la fonction de ce sous-système n'est plus remplie.
$\Phi_{1_i}(\underline{e})$	la fonction de structure Φ quand l'EB_i est certain (aussi notée $\Phi\left(\underline{e}_{-i}, e_i = 1\right)$)
$\Phi_{0_i}(\underline{e})$	la fonction de structure Φ quand l'EB_i est impossible (aussi notée $\Phi\left(\underline{e}_{-i}, e_i = 0\right)$)
R	le risque de référence ($= P(CI)$)
$R_{1,i}$	le risque quand l'événement i est certain ($= P(CI/EB_i) = P(\Phi_{1_i}(\underline{e}) = 1)$)
$R_{0,i}$	le risque quand l'événement i est impossible ($= P\left(CI/\overline{EB_i}\right) = P(\Phi_{0_i}(\underline{e}) = 1)$)
$\Delta_{TR;1,i}$	la valeur de la sous-estimation de $R_{1,i}$ due à la troncation du jeu de coupes
$\Delta_{TR;0,i}$	la valeur de la sous-estimation de $R_{0,i}$ due à la troncation du jeu de coupes

On introduit enfin la "fonction de risque", notée f_R, qui exprime le risque en fonction de la probabilité de chaque événement de base :

$$f_R\left(\underline{p}\right) = P(\Phi(\underline{e}) = 1)$$

avec $f_R : [0,1]^n \rightarrow \mathbb{R}^+$

2.1.2 Définition de la cohérence, de la criticité et de la défense en profondeur

Cette section présente les définitions des termes "défense en profondeur", "cohérence" et "criticité". Elles sont nécessaires à la bonne interprétation des facteurs d'importance.

Défense en profondeur

D'après le Groupe Consultatif Français de Sûreté [55], *"La Défense en Profondeur est la principale approche reconnue au niveau international qui permette d'atteindre les objectifs de sûreté fixés pour une installation nucléaire. Elle vise à compenser des défaillances matérielles ou humaines par des dispositions, situées à différents niveaux, incluant des barrières successives*

pour maîtriser les éventuels rejets accidentels de produits radioactifs dans l'environnement. Elle assure que les fonctions fondamentales de sûreté sont maîtrisées de manière satisfaisante, avec des marges suffisantes pour minimiser les risques liés à la défaillance de matériels et aux erreurs humaines, en prenant en compte les incertitudes associées à l'évaluation de ces défaillances et erreurs. Ce concept prévoit la surveillance et la protection des barrières par des dispositions appropriées et des mesures complémentaires de protection du public et de l'environnement pour le cas où ces barrières ne conserveraient pas leur pleine efficacité. " Pour synthétiser cette définition, on peut reprendre la définition du Mémento de la sûreté nucléaire [39] (équivalente à celle proposée par Sorensen dans son modèle structuraliste de la défense en profondeur [81]) : "*La défense en profondeur consiste à prendre en compte de façon systématique les défaillances de dispositions techniques, humaines ou organisationnelles et à s'en prémunir par des lignes de défense successives.*"

Ainsi, la défense en profondeur relativement à un événement i sera bonne si, lorsque cet événement est certain, le risque n'augmente pas trop.

Cohérence

Comme le rappelle Meng dans [66], une fonction de structure est dite cohérente si :

$$\begin{array}{l} \forall i \text{ et } \forall k, \quad \Phi_{1_i}\left(\underline{e}_k\right) \geq \Phi_{0_i}\left(\underline{e}_k\right) \\ \forall i,\ \exists k \text{ tel que : } \Phi_{1_i}\left(\underline{e}_k\right) > \Phi_{0_i}\left(\underline{e}_k\right) \end{array}$$

avec $\underline{e}_k$ un vecteur d'état.

Cela implique que la fonction de structure est monotone croissante pour toutes ses variables, que $\Phi\left(0^n\right) = 0$ et que $\Phi\left(1^n\right) = 1$. Si on associe à l'événement EB_i l'événement "défaillance du matériel i", on peut décrire la cohérence d'un système comme suit : "*Quand tous les matériels sont en panne, le système l'est aussi. Quand tous les matériels fonctionnent, le système fonctionne aussi. Un système en panne ne peut retourner à l'état de marche suite à la défaillance de l'un de ses composants. Chaque composant est critique pour au moins un état du système*".

Criticité

On dit d'un événement EB_i qu'il est critique relativement à un état k du système (noté $\left(\underline{e}_{k,-i}; e_i\right)$) si :

$$\left|\Phi_{1_i}\left(\underline{e}_k\right) - \Phi_{0_i}\left(\underline{e}_k\right)\right| = 1$$

Pour un état k du système donné, l'événement i est critique si l'état du système dépend de la valeur de e_i.

Pour un système cohérent, on peut définir la probabilité qu'un événement i soit critique, c'est-à-dire la probabilité d'être dans un état critique pour i, comme :

$$\begin{aligned} P\left(EB_i \; critique\right) &= P\left(\Phi_{1_i}\left(\underline{e}_k\right) - \Phi_{0_i}\left(\underline{e}_k\right) = 1\right) \\ &= E\left[\Phi_{1_i}\left(\underline{e}_k\right) - \Phi_{0_i}\left(\underline{e}_k\right)\right] \\ &= E\left[\Phi_{1_i}\left(\underline{e}_k\right)\right] - E\left[\Phi_{0_i}\left(\underline{e}_k\right)\right] \\ &= P\left(\Phi_{1_i}\left(\underline{e}_k\right) = 1\right) - P\left(\Phi_{0_i}\left(\underline{e}_k\right) = 0\right) \\ &= P\left(CI/EB_i\right) - P\left(CI/\overline{EB_i}\right) \end{aligned}$$

2.1.3 Facteurs d'importance probabilistes

La littérature sur les facteurs d'importance utilisés dans les EPS est abondante. Toutefois, pour un aperçu rapide des différents facteurs d'importance, on peut se reporter à [84] et [12]. Pour une lecture plus approfondie, on peut entre autres citer [42, 41, 94, 20, 64, 18, 63] qui exposent l'expression des facteurs d'importance, leur signification, leurs limites et leur applications dans le domaine du nucléaire.

Expression du risque en fonction d'un EB_i

Quel que soit l'EB_i considéré, Wall rappelle dans [99] qu'on peut toujours exprimer le risque par décomposition pivotale autour de EB_i. On obtient alors :

$$\begin{aligned} P(CI) &= P(EB_i)\cdot P(CI/EB_i) + \underbrace{P\left(\overline{EB_i}\right)}_{=1-P(EB_i)} \cdot P\left(CI/\overline{EB_i}\right) \\ &= P(EB_i)\cdot \underbrace{\left(P(CI/EB_i) - P\left(CI/\overline{EB_i}\right)\right)}_{\text{noté } a_i} + \underbrace{P\left(CI/\overline{EB_i}\right)}_{\text{noté } b_i} \end{aligned}$$

On retrouve alors l'expression du risque de référence en fonction de la probabilité d'un de ses EB [99], qui est :

$$P(CI) = a_i \cdot p_i + b_i$$

avec :

$$P(CI/EB_i) = a_i + b_i$$
$$P\left(CI/\overline{EB_i}\right) = b_i$$

Les valeurs a_i et b_i peuvent être approximées au moyen d'un développement de Poincaré à l'ordre 1 comme :

$$a_i \approx \sum_{EB_i \in CM_j} \frac{P(CM_j)}{p_i} \qquad b_i \approx \sum_{EB_i \notin CM_k} P(CM_k)$$

C'est à dire que a_i est approximé par la somme de la probabilité d'occurrence des coupes contenant EB_i et que b_i est approximé par la somme de la probabilité d'occurrence des coupes ne contenant pas EB_i. La figure 1.9 représente cette relation affine entre p_i et $P(CI)$. Comme le

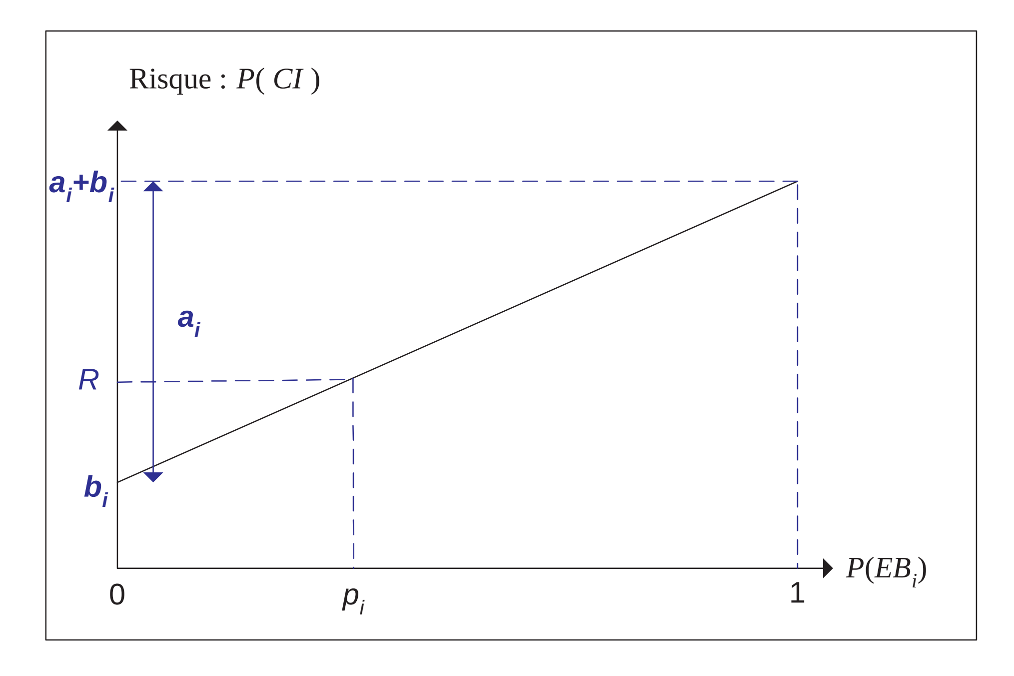


FIG. 1.9 – *Risque en fonction de la probabilité de l'EB_i*

fait remarquer [42], la pente de cette droite (le paramètre a_i) renseigne sur le niveau de défense en profondeur relativement à l'événement EB_i. En effet, plus la pente est forte (a_i élevé) plus, pour un accroissement donné de la probabilité p_i, l'accroissement du risque est important, donc moins la défense en profondeur relativement à l'événement i est bonne.

De plus, comme on l'a vu dans la section 2.1.2, puisqu'on formule l'hypothèse que la fonction de structure est cohérente, la valeur a_i peut être comprise comme la probabilité que la centrale soit dans un état critique pour l'EB_i. En effet : $a_i = P(CI/EB_i) - P\left(CI/\overline{EB_i}\right)$.

Les principaux facteurs d'importance probabilistes

L'indicateur de Birnbaum : C'est l'une des premières mesures d'importance qui ont été définies [11]. Elle s'exprime comme la différence entre le risque sachant que EB_i s'est produit et le risque sachant que cet événement ne peut pas se produire. Sa formulation mathématique est :

$$I_B\left(EB_i\right) = P\left(CI/EB_i\right) - P\left(CI/\overline{EB_i}\right) = R_{1,i} - R_{0,i} = \frac{\partial f_R\left(\underline{p}\right)}{\partial p_i}$$

Si on reprend l'expression du risque de Wall, on voit alors que $I_B\left(EB_i\right) = a_i$. Donc, comme précédemment, on en déduit que sous l'hypothèse de cohérence de la fonction de structure communément acceptée dans les EPS, l'indicateur de Birnbaum d'EB_i correspond à la probabilité que cet événement soit critique [12].

Le Facteur d'Accroissement de risque (FAR) : Le Facteur d'Accroissement de Risque (FAR) de EB_i se définit comme l'augmentation relative du risque qu'impliquerait une occurrence certaine de l'événement i étudié. Le FAR peut donc s'exprimer comme :

$$FAR\left(EB_i\right) = \frac{P\left(CI/EB_i\right) - P\left(CI\right)}{P\left(CI\right)} = \frac{R_{1,i} - R}{R} = \frac{\frac{\partial f_R\left(\underline{p}\right)}{\partial p_i} \cdot \left(1 - p_i\right)}{f_R\left(\underline{p}\right)}$$

En reprenant l'expression de Wall, on voit alors que :

$$FAR\left(EB_i\right) = \frac{a_i \cdot \left(1 - p_i\right)}{R}$$

Sous l'hypothèse de cohérence de la fonction de structure, le FAR correspond alors à la probabilité que la centrale soit dans un état critique pour EB_i et que EB_i ne se réalise pas. C'est donc le quotient de la probabilité que la non-défaillance de i empêche la fusion par R.

Le "Risk Increase Factor" (RIF) ou le "Risk Achievment Worth" (RAW) : Le Risk Increase Factor de EB_i se définit comme le facteur d'augmentation du risque[8] qu'impliquerait une occurrence certaine de l'événement i étudié. Ce facteur d'importance est aussi appelé "Risk Achievment Worth" (RAW). Le RIF peut donc s'exprimer comme :

$$RIF\left(EB_i\right) = RAW\left(EB_i\right) = \frac{P\left(CI/EB_i\right)}{P\left(CI\right)} = \frac{R_{1,i}}{R}$$

En reprenant l'expression de Wall, on voit alors que :

$$RIF\left(EB_i\right) = \frac{a_i + b_i}{R}$$

Le Facteur de Sensibilité (FS) : Le facteur de sensibilité exprime l'augmentation relative de risque résultant d'une variation Δ_{p_i} de la probabilité d'occurrence d'EB_i.
Le FS peut donc s'exprimer comme :

$$FS\left(EB_i, \Delta_{p_i}\right) = \frac{P\left(CI\right)_{\text{avec } p_i' = p_i + \Delta_{p_i}} - P\left(CI\right)}{P\left(CI\right)} = \frac{\Delta_{p_i} \cdot \left(R_{1,i} - R_{0,i}\right)}{R} = \frac{\frac{\partial f_R\left(\underline{p}\right)}{\partial p_i} \cdot \Delta_{p_i}}{f_R\left(\underline{p}\right)}$$

En reprenant l'expression de Wall, on voit alors que :

$$FS\left(EB_i, \Delta_{p_i}\right) = \frac{a_i \cdot \Delta_{p_i}}{R}$$

[8] Le FAR au contraire est un facteur d'augmentation relatif

Le Facteur de Diminution de Risque (FDR) : Le Facteur de Diminution de Risque (FDR) de EB_i se définit comme la diminution relative du risque qu'impliquerait une occurrence rendue impossible de l'événement i étudié. Le FDR peut donc s'exprimer comme :

$$FDR\left(EB_i\right) = \frac{P\left(CI\right) - P\left(CI/\overline{EB_i}\right)}{P\left(CI\right)} = \frac{R - R_{0,i}}{R} = \frac{\dfrac{\partial f_R\left(\underline{p}\right)}{\partial p_i} \cdot p_i}{f_R\left(\underline{p}\right)}$$

En reprenant l'expression de Wall, on voit alors que :

$$FDR\left(EB_i\right) = \frac{a_i \cdot p_i}{R}$$

Sous l'hypothèse de cohérence de la fonction de structure, le FDR correspond à la probabilité que la centrale soit dans un état critique pour EB_i et que EB_i se réalise. C'est donc la probabilité que la défaillance de i provoque la fusion.

Puisque le risque est une fonction affine de la probabilité p_i d'occurrence de l'événement i, la valeur du FDR de EB_i correspond à l'accroissement de risque relatif lorsque la probabilité d'occurrence de EB_i est doublée [42]. En effet,

$$FDR = \frac{R - R_{0,i}}{R} = \frac{a_i \cdot p_i}{R} = \frac{\overbrace{\left(a_i \cdot 2 \cdot p_i + b_i\right)}^{R_{p'_i = 2\cdot p_i} = a_i \cdot p'_i + b_i} - \left(a_i \cdot p_i + b_i\right)}{R} = \frac{R_{p'_i = 2\cdot p_i} - R}{R} = FS\left(EB_i, \Delta_{p_i}\right)$$

avec $\Delta_{p_i} = p_i$ et $R_{p'_i = 2\cdot p_i}$ le risque lorsque la probabilité d'occurrence de EB_i est deux fois supérieure à sa probabilité de référence.

Le Facteur de Vesely Fussel (VF) : Le Facteur de Vesely Fussel (VF) de EB_i se définit comme la probabilité qu'une coupe contenant EB_i soit réalisée sachant que l'événement CI s'est produit. Le VF peut donc s'exprimer comme :

$$VF\left(EB_i\right) = P\left(\left(\bigcup_{EB_i \in CM_j} CM_j\right)/CI\right) = \frac{P\left(CI \cap \bigcup_{EB_i \in CM_j} CM_j\right)}{P\left(CI\right)} = \frac{P\left(\bigcup_{EB_i \in CM_j} CM_j\right)}{P\left(CI\right)}$$

Si $R_{1,i}$, $R_{0,i}$, R et $P\left(\bigcup_{EB_i \in CM_j} CM_j\right)$ sont approximés par la formule de Poincaré à l'ordre 1, alors le FDR et VF sont calculés de la même façon comme :

$$VF\left(EB_i\right) \underset{\substack{\text{événements}\\ \text{rares}}}{\approx} FDR\left(EB_i\right) \underset{\substack{\text{événements}\\ \text{rares}}}{\approx} \frac{\sum_{EB_i \in CM_j} P\left(CM_j\right)}{R}$$

Le "Risk Decrease Factor" (RDF) ou le "Risk Reduction Worth" (RRW) : Le Risk Decrease Factor de EB_i se définit comme le facteur de diminution du risque qu'impliquerait une occurrence impossible de l'événement i étudié. Ce facteur d'importance est aussi appelé "Risk Reduction Worth" (RRW). Le RDF peut donc s'exprimer comme :

$$RDF\left(EB_i\right) = RRW\left(EB_i\right) = \frac{P\left(CI\right)}{P\left(CI/\overline{EB_i}\right)} = \frac{R}{R_{0,i}}$$

En reprenant l'expression de Wall, on voit alors que :

$$RDF\left(EB_i\right) = \frac{R}{b_i}$$

La "Differential Importance Measure" (DIM) : Cet indicateur, établi par Borgonovo en 2001 [13], est le dernier à avoir été introduit. Pour présenter ce facteur DIM, il faut avoir recours à la notion de paramètre. On définit la fonction de passage g qui permet, à partir des paramètres x_j, d'obtenir les probabilités p_i telles que :

$$g \ : \ \underline{x} \rightarrow \underline{p} \text{ avec } g\left(\underline{x}\right) = \underline{p}$$

On notera $f_{R,g}$ la fonction exprimant le risque en fonction des paramètres. $\underline{x}$ est un vecteur à valeurs dans $\mathbb{R}^m$. g est une fonction de $\mathbb{R}^m$ dans $[0,1]^n$ et

$$f_{R,g}\left(\underline{x}\right) = f_R\left(\underline{p}\right) = f_R\left(g\left(\underline{x}\right)\right)$$

1. *Expression de ce facteur à partir des paramètres de la fonction du risque :*
   Le facteur DIM doit être interprété comme (cf. [13]) "*la fraction du changement total de $R_{\underline{x}}$ due au changement de paramètre x_i*" dans le cadre de petits changements autour de leur valeur de référence. Ce facteur peut s'exprimer suivant deux hypothèses :

   H1 : tous les paramètres varient de la même petite valeur
   H2 : tous les paramètres varient suivant le même (petit) pourcentage

   Sous H1, le facteur DIM vaut : $DIM\left(x_i\right) = \left.\dfrac{\partial f_{R,g}\left(\underline{x}\right)}{\partial x_i} \Bigg/ \sum_{j=1}^{m} \dfrac{\partial f_{R,g}\left(\underline{x}\right)}{\partial x_j}\right|_{\underline{x}_{ref.}}$

   Sous H2, le facteur DIM vaut : $DIM\left(x_i\right) = \left.\dfrac{\partial f_{R,g}\left(\underline{x}\right)}{\partial x_i} \cdot x_i \Bigg/ \sum_{j=1}^{m} \dfrac{\partial f_{R,g}\left(\underline{x}\right)}{\partial x_j} \cdot x_j\right|_{\underline{x}_{ref.}}$

   avec $\underline{x}_{ref.}$ le vecteur contenant les valeurs de référence des paramètres.

2. *Expression de ce facteur à partir des probabilités d'occurrence des événements de base :*
   Lorsqu'on considère les probabilités de chacun des EB et non plus leurs paramètres, les hypothèses H1 et H2 deviennent :

   H1 : toutes les probabilités varient de la même petite valeur
   H2 : toutes les probabilités varient suivant le même (petit) pourcentage

   Sous H1, le facteur DIM vaut : $DIM\left(p_i\right) = \left.\dfrac{\partial f_R\left(\underline{p}\right)}{\partial p_i} \Bigg/ \sum_{j=1}^{n} \dfrac{\partial f_R\left(\underline{p}\right)}{\partial p_j}\right|_{\underline{p}_{ref.}}$

   Sous H2, le facteur DIM vaut : $DIM\left(p_i\right) = \left.\dfrac{\partial f_R\left(\underline{p}\right)}{\partial p_i} \cdot p_i \Bigg/ \sum_{j=1}^{n} \dfrac{\partial f_R\left(\underline{p}\right)}{\partial p_j} \cdot p_j\right|_{\underline{p}_{ref.}}$

   avec $\underline{p}_{ref.}$ le vecteur contenant les probabilités de référence des EB.

Additivité
Une des propriétés intéressantes de ce facteur est qu'il est additif. En effet, si on prend l'exemple du facteur DIM basé sur les probabilités avec l'hypothèse H2, le facteur de plusieurs événements de base est défini comme :

$$DIM\left(p_1, p_2, \ldots, p_i, \ldots, p_k\right) = \left.\sum_{1 \leq i \leq k} \frac{\partial f_R\left(\underline{p}\right)}{\partial p_i} \cdot p_i \Bigg/ \sum_{j=1}^{n} \frac{\partial f_R\left(\underline{p}\right)}{\partial p_j} \cdot p_j\right|_{\underline{p}_0}$$

De manière plus générale, $DIM\left(p_1, p_2, \ldots, p_i, \ldots, p_k\right) = \sum_{1 \leq i \leq k} DIM\left(p_i\right)$.

Quels que soient le ou les paramètres (ou probabilités) considérés, leur facteur DIM nous renseigne sur la fraction d'évolution élémentaire causée par ce ou ces paramètres (ou probabilités).

Ainsi, si on considère toutes les probabilités, $DIM\left(p_1, p_2, \ldots, p_n\right) = 1$

Correspondance avec les autres facteurs d'importance :
Quand le facteur DIM est exprimé à partir des probabilités d'occurrence des EB, que l'hypothèse H2 est utilisée et que tous les EB sont considérés, on a :

$$DIM\left(p_i\right) = \frac{FDR\left(EB_i\right)}{\sum_{j=1}^{n} FDR\left(EB_j\right)}$$

Quand le facteur DIM est exprimé à partir des probabilités d'occurrence des EB, que l'hypothèse H1 est utilisée et que tous les EB sont considérés, on a :

$$DIM\left(p_i\right) = \frac{I_B\left(EB_i\right)}{\sum_{j=1}^{n} I_B\left(EB_j\right)}$$

Relation entre les différents facteurs d'importance

Suite à la présentation dans le tableau 1.1 de ces principaux facteurs d'importance, on se rend compte qu'ils peuvent tous être exprimés à partir de $R_{1,i}$, de $R_{0,i}$ et de R, excepté pour le VF, où une approximation est requise, et pour le facteur DIM, lorsqu'il est calculé pour les paramètres.
Déterminer les valeurs de $R_{1,i}$, de $R_{0,i}$ et de R suffit donc pour calculer tous les principaux facteurs d'importance utilisés dans les EPS.

Facteur d'importance	avec $R_{1,i}$ et $R_{0,i}$	avec a_i et b_i
$DIM_{H1}\left(p_i\right)$	$DIM_{H1}\left(p_i\right) = R_{1,i} - R_{0,i} \Big/ \sum_{j=1}^{n} R_{1,j} - R_{0,j}\Big\|_{\underline{p}_0}$	$DIM_{H1}\left(p_i\right) = a_i \Big/ \sum_{j=1}^{n} a_j \Big\|_{\underline{p}_0}$
$DIM_{H2}\left(p_i\right)$	$DIM_{H2}\left(p_i\right) = \left(R_{1,i} - R_{0,i}\right) \cdot p_i \Big/ \sum_{j=1}^{n} \left(R_{1,j} - R_{0,j}\right) \cdot p_i \Big\|_{\underline{p}_0}$	$DIM_{H2}\left(p_i\right) = a_i \cdot p_i \Big/ \sum_{j=1}^{n} a_j \cdot p_i \Big\|_{\underline{p}_0}$
$I_B\left(EB_i\right)$	$R_{1,i} - R_{0,i}$	a_i
$FAR\left(EB_i\right)$	$\frac{R_{1,i} - R}{R}$	$\frac{\left(1 - p_i\right) \cdot a_i}{R}$
$RIF\left(EB_i\right)$	$\frac{R_{1,i}}{R}$	$\frac{a_i - b_i}{R}$
$FS\left(EB_i\right)$	$\frac{\left(R_{1,i} - R_{0,i}\right) \Delta_{p_i}}{R}$	$\frac{\Delta_{p_i} \cdot a_i}{R}$
$FDR\left(EB_i\right)$	$\frac{R - R_{0,i}}{R}$	$\frac{p_i \cdot a_i}{R}$
$VF\left(EB_i\right)$	$\underset{\text{événements rares}}{\approx} \frac{R - R_{0,i}}{R}$	$\underset{\text{événements rares}}{\approx} \frac{p_i \cdot a_i}{R}$
$RDF\left(EB_i\right)$	$\frac{R}{R_{0,i}}$	$\frac{R}{p_i \cdot a_i}$

TAB. 1.1 – *Tableau de synthèse de l'expression mathématique des facteurs d'importance*

Exemple du facteur de sensibilité : Comme tous les facteurs d'importance sont liés, on peut les exprimer les uns à partir des autres. C'est par exemple le cas du facteur de sensibilité, qui peut être exprimé comme : $FS\left(EB_i\right) = \Delta_{p_i} \cdot \left(FAR\left(EB_i\right) + FDR\left(EB_i\right)\right)$

Classification des facteurs d'importance

Les différents facteurs d'importance probabilistes peuvent être classés en fonction de l'information qu'ils fournissent [84].

Le FAR, le RIF et l'indicateur de Birnbaum d'un événement i peuvent être considérés comme des indicateurs mesurant le niveau de défense en profondeur relativement à i. En effet, en estimant le risque ou l'accroissement de risque lorsque l'occurrence de l'événement i est certaine, le FAR et le RIF renseignent sur le niveau de protection face à l'occurrence de cet événement quelle qu'en soit la probabilité d'occurrence. L'indicateur de Birnbaum lui, en donnant la probabilité que l'événement i soit critique, renseigne aussi sur le niveau de défense en profondeur dans la mesure où un événement qui est souvent critique est un événement face auquel on est mal protégé. Ainsi Youngblood, dans [100], considère que ces trois facteurs d'importance servent à détecter les événements "*significatifs pour la sûreté*".

Le FDR et le facteur de Vesely Fussel[9] renseignent eux sur la contribution au risque d'un événement i. En effet,on a vu que, si le système est cohérent, le FDR et, à l'approximation des événements rares près, le VF équivalent à la probabilité que l'événement i soit critique et réalisé, divisée par le risque. La probabilité qu'il soit "critique et réalisé" renseigne donc sur sa contribution au risque. Ainsi Youngblood, dans [100], considère que ces deux facteurs d'importance servent à détecter les événements "*significatifs pour le risque*".

Il est toutefois à noter que le FDR peut aussi être compris comme un indicateur permettant le diagnostic. En effet, si la fonction de structure est cohérente, le FDR nous donne la probabilité que l'occurrence de l'événement i ait provoqué l'événement CI sachant qu'il est réalisé. Si on assimile l'événement i à un matériel i, et l'événement CI à la défaillance du système étudié, le FDR de chaque matériel nous donne la probabilité qu'elle ait été causée par i sachant la défaillance du système, donc la probabilité que le système retourne dans un état de marche grâce à la réparation de i.

Dans les EPS, l'aspect diagnostic n'est que peu utile. En effet, on n'envisage pas, ou très peu, de réparations dans ces modèles et si l'événement CI est réalisé, il est irréversible. Si on prend l'exemple des EPS de niveau 1, même si la fonction booléenne indique que la remise en marche d'un composant i devrait annuler l'événement $FUSION$, dans la réalité, une fois que la fusion est avérée, aucune réparation d'aucun composant ne peut l'annuler. On peut seulement chercher à en réduire les conséquences.

2.1.4 Facteurs d'importance structuraux

En l'absence de probabilités d'occurrence des événements de base, les quantités $R_{1,i}$, $R_{0,i}$ et R ne peuvent plus être calculées. L'ensemble des définitions exposées dans la section précédente est donc inutilisable. Des facteurs d'importance dits "structuraux" ont été proposés. Ils se basent sur la structure (d'où leur nom) de la fonction de structure et non sur la probabilité d'occurrence de l'événement qu'elle modélise (dans notre cas l'événement CI). Pour un tour d'horizon de ces facteurs, on peut citer Boland [12] et Meng [66, 65]. La présentation de la version structurelle de l'indicateur de Birnbaum et le classement de Butler donnent un aperçu de ces indicateurs.

Indicateur de Birnbaum, définition structurelle

Soit Φ la fonction de structure, et $\underline{e}$ le vecteur d'état. Il existe 2^{n-1} vecteurs différents $\underline{e}_{-i}$ avec n le nombre de dimensions de $\underline{e}$[10]. La proportion de ces vecteurs qui sont critiques nous donne l'indicateur de Birnbaum structurel :

$$I_{B,struct.}\left(EB_i\right) = \frac{Card\left[\underline{e} : \Phi\left(\underline{e}_{-i}, e_i = 1\right) > \Phi\left(\underline{e}_{-i}, e_i = 0\right)\right]}{2^{n-1}}$$

[9] ainsi que le RDF dans une moindre mesure car il peut être rattaché au FDR

[10] n le nombre d'événements élémentaires intervenant dans la fonction de structure.

Cet indicateur a comme limite importante le fait que l'ensemble $Card\left[\underline{e} : \Phi\left(\underline{e}_{-i}, e_i = 1\right) > \Phi\left(\underline{e}_{-i}, e_i = 0\right)\right]$ ne peut être calculé que pour de petits systèmes. L'explosion combinatoire ne permet pas de le calculer dans une EPS.

Mesure structurelle de Barlow et Proschan
Barlow et Proschan ont défini l'indicateur structurel I_{BP} comme :

$$I_{BP,\Phi}\left(EB_i\right) = \frac{1}{n} \cdot \sum_{r=1}^{n} \frac{n_r\left(i\right)}{C_{n-1}^{r-1}}$$

avec :

$n_r\left(i\right)$ le nombre de coupes contenant EB_i de taille r

n le nombre d'événements dans le modèle

Classification de Butler
Butler a proposé une méthode de classement des composants basée sur les coupes minimales. Ainsi, $d_{i,k}$ est défini comme le nombre de coupes d'ordre k contenant EB_i. On peut alors définir le vecteur $\underline{d}_i$ comme $\underline{d}_i = (d_{i,1}, d_{i,2}, \ldots, d_{i,n})$ avec n le nombre d'EB du modèle. Un événement i est plus important qu'un événement j si :

$$\underline{d}_i \succ \underline{d}_j$$

avec $\succ$ l'opérateur de comparaison lexicographique. C'est à dire qu'on compare les deux premiers termes. S'ils sont égaux, on compare les seconds et ainsi de suite. Ainsi l'événement i est plus important que l'événement j si :

$$d_{i,l} = d_{j,l} \forall l \in [1;k] \text{ et } d_{i,k+1} > d_{j,k+1} \text{ avec } k < n$$

2.2 Facteurs d'importance et défaillance de causes communes

Comme on l'a vu au paragraphe 1.3.3 du chapitre 1, les événements de base interdépendants sont modélisés au moyen d'EB_{DCC}. Dans la mesure où RSW génère automatiquement plusieurs EB_{DCC} pour un même événement de base, plusieurs facteurs d'importance seront automatiquement calculés pour chacun de ces EB_{DCC} alors qu'ils se rapportent tous à un seul événement. L'interprétation de ces facteurs d'importance est alors moins simple.

Pour étudier un EB appartenant à un groupe DCC, on pourra chercher à connaître l'importance de la défaillance intrinsèque d'un composant i, l'importance de la défaillance du fait d'une cause commune du composant i et d'autres composant du groupe, ou encore l'importance de la défaillance du composant i quelle qu'en soit la cause.

2.2.1 Type de causes que l'on peut considérer et probabilité associée avec le modèle MGL

Comme l'expose l'article [87] écrit en partenariat entre l'UTT et EDF R&D, quatre types de causes peuvent être considérés pour la défaillance d'un composant i appartenant à un groupe DCC de taille m inférieure ou égale à quatre :

1. la défaillance intrinsèque d'un composant i. L'événement considéré est alors : $EB_{int,i}$
2. l'occurrence d'une défaillance de causes communes impliquant le composant i. L'événement considéré est alors :

$$\left(\bigcup_{i \neq j} EB_{DCC;i,j}\right) \cup \left(\bigcup_{i \neq j, i \neq k, j \neq k} EB_{DCC;i,j,k}\right) \cup EB_{DCC;tous}$$

3. la défaillance du composant sans qu'on en connaisse la cause. L'événement considéré est alors :

$$EB_{int,i} \cup \left(\bigcup_{i \neq j} EB_{DCC;i,j} \right) \cup \left(\bigcup_{i \neq j, i \neq k, j \neq k} EB_{DCC;i,j,k} \right) \cup EB_{DCC;tous}$$

4. la non-disponibilité du composant i pour maintenance. Dans ce cas, il peut toujours être affecté par des défaillances de causes communes. On n'est pas dans le cas d'une défaillance intrinsèque.

2.2.2 Calcul des facteurs d'importance associés aux différentes causes

Comme on l'a vu au paragraphe 2.1.3 du chapitre 1, tous les facteurs d'importance courants peuvent être calculés à partir des valeurs $R_{1,i}$, $R_{0,i}$ et R. Si on est capable d'exprimer ces trois quantités pour chacun des événements listés précédemment, on pourra calculer leurs facteurs d'importance. R étant déjà connu, il reste donc à calculer $R_{1,i}$ et $R_{0,i}$.

Les différents événements d'un groupe DCC (les EB_{DCC} et les $EB_{int,i}$) sont incompatibles. Il n'y a donc aucune coupe contenant deux EB_{DCC} issus d'un même groupe. On peut donc écrire pour un groupe DCC d'ordre 4 ($m \leq 4$) et pour un EB_i appartenant à ce groupe :

$$CI = \Bigg[\overbrace{\left(\bigcup_{EB_{int,i} \in CM_k} CM_k \right)}^{\text{les coupes contenant } EB_{int,i}} \oplus \left(\bigoplus_{\substack{j=1,\\ j \neq i}}^{m} \left(\bigcup_{EB_{DCC;i,j} \in CM_k} CM_k \right) \right) \oplus \left(\bigoplus_{j \neq l \neq i} \left(\bigcup_{EB_{DCC;i,j,l} \in CM_k} CM_k \right) \right)$$
$$\oplus \left(\bigcup_{EB_{DCC;tous} \in CM_k} CM_k \right) \oplus \left(\bigoplus_{\substack{\text{Tous les EB} \\ \text{du groupe DCC} \\ \text{ne contenant pas } i}} \left(\bigcup_{EB_{DCC \notin i} \in CM_k} CM_k \right) \right) \Bigg]$$
$$\cup \underbrace{\left(\bigcup_{EB_i \text{ pas dans } CM_k} CM_k \right)}_{\substack{\text{les coupes ne contenant aucun EB} \\ \text{lié au groupe DCC}}}$$

avec l'opérateur $\oplus$ qui correspond au "OU exclusif".

Pour condenser la formule précédente on définit les notations suivantes :

$A_{int,i}$ l'événement $\left(\bigcup_{EB_{int,i} \in CM_k} CM_k \right)$ qui correspond à l'union des coupes contenant $EB_{int,i}$

$A_{DCC;i,j}$ l'événement $\left(\bigcup_{EB_{DCC.i,j} \in CM_k} CM_k \right)$ qui correspond à l'union des coupes contenant $EB_{DCC;i,j}$

$A_{DCC;i,j,k}$ l'événement $\left(\bigcup_{EB_{DCC;i,j,l} \in CM_k} CM_k \right)$ qui correspond à l'union des coupes contenant $EB_{DCC;i,j,l}$

$A_{DCC;tous}$ l'événement $\left(\bigcup_{EB_{DCC;tous} \in CM_k} CM_k \right)$ qui correspond à l'union des coupes contenant $EB_{DCC;tous}$

$B_{DCC;pas\ i}$ l'événement $\bigoplus_{\substack{\text{Tous les EB}\\ \text{du groupe DCC}\\ \text{ne contenant pas } i}} \left(\bigcup_{EB_{DCC \notin i} \in CM_k} CM_k \right)$ qui correspond à l'union de toutes les coupes contenant un EB du groupe DCC mais n'impliquant pas la défaillance de i

B_i l'événement $\left(\bigcup_{EB_i \text{ pas dans } CM_k} CM_k \right)$ qui correspond à l'union des coupes ne contenant auncun EB du groupe DCC

Puisque les différents événements d'un groupe DCC (les EB_{DCC} et les $EB_{int,i}$) sont incompatibles, si on s'intéresse à un événement de base i appartenant à un groupe DCC d'une taille d'au plus quatre, on peut écrire $P(CI)$ comme :

$$P(CI) =$$
$$P(A_{int,i}) + \sum_{\substack{j=1,\\ j \neq i}}^{m} P(A_{DCC;i,j}) + \sum_{j \neq l \neq i} P(A_{DCC;i,j,l}) + P(A_{DCC;tous}) + P(B_{DCC;pas\ i}) + P(B_i)$$
$$-P(A_{int,i} \cap B_i) - \sum_{\substack{j=1,\\ j \neq i}}^{m} P(A_{DCC;i,j} \cap B_i) - \sum_{j \neq l \neq i} P(A_{DCC;i,j,l} \cap B_i) - P(A_{DCC;tous} \cap B_i)$$
$$-P(B_{DCC;pas\ i} \cap B_i)$$

On résume cette expression du risque de référence en introduisant les quantités $a_{int,i}$, $a_{DCC;i,j}$, $a_{DCC;i,j,k}$, $a_{DCC;tous}$, $b_{DCC;pas\ i}$ et b_i. Le risque de référence relativement à l'EB_i pour un groupe DCC de taille inférieure ou égale à 4 est alors exprimé comme :

$$\begin{aligned} R = \ & a_{int,i} \cdot p_{int,i} + \sum_{j=1, i \neq j}^{m} a_{DCC;i,j} \cdot p_{DCC;i,j} \\ & + \sum_{i \neq j, i \neq k, j \neq k} a_{DCC;i,j,k} \cdot p_{DCC;i,j,k} + a_{DCC,tous} \cdot p_{DCC;tous} + b_{DCC;pas\ i} + b_i \\ R = \ & a_{int,i} \cdot (1-\beta) \cdot Q_{tot} + \sum_{j=1, i \neq j}^{m} a_{DCC;i,j} \cdot \frac{\beta \cdot (1-\gamma) \cdot Q_{tot}}{k_2} \\ & + \sum_{i \neq j, i \neq k, j \neq k} a_{DCC;i,j,k} \cdot \frac{\beta \cdot \gamma (1-\delta) \cdot Q_{tot}}{k_3} + a_{DCC,tous} \cdot \beta \cdot \gamma \cdot \delta \cdot Q_{tot} + b_{DCC;pas\ i} + b_i \end{aligned}$$

$$k_2 = \begin{cases} m-1 \text{ si } m > 2 \\ 1 \text{ sinon} \end{cases} \quad \text{et} \quad k_3 = \begin{cases} m-1 \text{ si } m = 4 \\ 1 \text{ sinon} \end{cases} \quad \begin{matrix} \text{et} & \gamma = 0 \text{ si } m = 2 \\ \text{et} & \delta = 0 \text{ si } m = 3 \end{matrix}$$

avec :

$a_{int,i}$ la probabilité $P(A_{int,i}/EB_{int,i}) - P(A_{int,i} \cap B_i/EB_{int,i})$

$a_{DCC;i,j}$ la probabilité $P(A_{DCC;i,j}/EB_{DCC;i,j}) - P(A_{DCC;i,j} \cap B_i/EB_{DCC;i,j})$

$a_{DCC;i,j,k}$ la probabilité $P(A_{DCC;i,j,k}/EB_{DCC;i,j,k}) - P(A_{DCC;i,j,k} \cap B_i/EB_{DCC;i,j,k})$

$a_{DCC;tous}$ la probabilité $P(A_{DCC;tous}/EB_{DCC;tous}) - P(A_{DCC;tous} \cap B_i/EB_{DCC;tous})$

$b_{DCC;pas\ i}$ la probabilité $P(B_{DCC;pas\ i}) - P(B_{DCC;pas\ i} \cap B_i)$

b_i la probabilité $P(B_i)$

Calcul de $R_{1,i}$ et de $R_{0,i}$

On suppose que le groupe DCC étudié contient au plus quatre EB. On pose

$$k_2 = \begin{cases} m-1 \text{ si } m > 2 \\ 1 \text{ sinon} \end{cases} \quad \text{et} \quad k_3 = \begin{cases} m-1 \text{ si } m > 3 \\ 1 \text{ sinon} \end{cases} \quad \begin{matrix} \text{et} & \gamma = 0 \text{ si } m = 2 \\ \text{et} & \delta = 0 \text{ si } m = 3 \end{matrix}$$

On peut alors exprimer $R_{1,i}$ et $R_{0,i}$ pour les différents événements considérés.

1. *Défaillance intrinsèque*
   Les événements DCC sont incompatibles, donc si l'événement $EB_{int,i}$ est certain, tous les

EB_{DCC} contenant i sont impossibles.
$R_{1,(int,i)}$ s'exprime donc comme :

$$R_{1,(int,i)} = a_{int,i} + b_i$$

Et $R_{0,(int,i)}$ s'exprime donc comme :

$$\begin{aligned} R_{0,(int,i)} = & \sum_{j=1,i\neq j}^{m} a_{DCC;i,j} \cdot \frac{\beta \cdot (1-\gamma) \cdot Q_{tot}}{k_2} + \sum_{i\neq j,i\neq k,j\neq k} a_{DCC;i,j,k} \cdot \frac{\beta \cdot \gamma\,(1-\delta) \cdot Q_{tot}}{k_3} \\ & + a_{DCC,tous} \cdot \beta \cdot \gamma \cdot \delta \cdot Q_{tot} + b_{DCC;pas\ i} + b_i \end{aligned}$$

2. *Défaillance de causes communes*
Lorsqu'on veut calculer $R_{1,(DCC;i,\bullet)}$, on sait qu'un des événements DCC incluant la défaillance de i s'est produit. Il en découle que :
- $\beta = 1$,
- $Q_{tot} = 1$,
On en déduit que la probabilité d'une défaillance intrinsèque est nulle ($(1-\beta) \cdot Q_{tot} = 0$) et que la probabilité d'occurrence des EB_{DCC} est divisée par $(1-\beta) \cdot Q_{tot}$ par rapport à leur probabilité de référence. $R_{1,(DCC;i,\bullet)}$ s'exprime donc comme :

$$\begin{aligned} R_{1,(DCC;i,\bullet)} = & \sum_{j=1,i\neq j}^{m} a_{DCC;i,j} \cdot \frac{(1-\gamma)}{k_2} \\ & + \sum_{i\neq j,i\neq k,j\neq k} a_{DCC;i,j,k} \cdot \frac{\gamma\,(1-\delta)}{k_3} + a_{DCC,tous} \cdot \gamma \cdot \delta + b_i \end{aligned}$$

Lorsqu'on calcule $R_{0,(DCC;i,\bullet)}$, on sait qu'aucun événement DCC ne peut se produire. On a donc :

$$R_{0,(DCC;i,\bullet)} = a_{int,i} \cdot (1-\beta) \cdot Q_{tot} + b_{DCC;pas\ i} + b_i$$

3. *Défaillance de cause inconnue*
Dans ce cas, lorsqu'on calcule $R_{1,i}$, la seule information connue est que l'occurrence de EB_i est certaine, ce qui implique que $Q_{tot} = 1$. On a donc :

$$\begin{aligned} R_{1,i} = & \ a_{int,i} \cdot (1-\beta) + \sum_{j=1,i\neq j}^{m} a_{DCC;i,j} \cdot \frac{\beta \cdot (1-\gamma)}{k_2} \\ & + \sum_{i\neq j,i\neq k,j\neq k} a_{DCC;i,j,k} \cdot \frac{\beta \cdot \gamma\,(1-\delta)}{k_3} + a_{DCC,tous} \cdot \beta \cdot \gamma \cdot \delta + b_i \end{aligned}$$

Lorsqu'on calcule $R_{0,i}$, on considère que l'événement i ne peut pas se réaliser, quelle que soit la cause étudiée. On obtient donc :

$$R_{0,i} = b_i + b_{DCC;pas\ i}$$

4. *Indisponibilité pour cause de maintenance*
Bien que l'événement i soit réalisé du fait de la maintenance, les DCC pouvant impacter les autres matériels du groupe sont toujours considérées. On a alors $R_{1,(maint.,i)}$ tel que :

$$\begin{aligned} R_{1,(maint.,i)} = & \ a_{int,i} + \sum_{j=1,i\neq j}^{m} a_{DCC;i,j} \cdot \frac{\beta \cdot (1-\gamma) \cdot Q_{tot}}{k_2} + b_{DCC;pas\ i} \\ & + \sum_{\substack{i\neq j,i\neq k,\\ j\neq k}} a_{DCC;i,j,k} \cdot \frac{\beta \cdot \gamma\,(1-\delta) \cdot Q_{tot}}{k_3} + a_{DCC,tous} \cdot \beta \cdot \gamma \cdot \delta \cdot Q_{tot} + b_i \end{aligned}$$

Exemple du FAR

Il est à noter que, lorsque RSW modélise des DCC, il ne prend pas en compte le fait que certains de ces événements DCC sont incompatibles. Comme on l'a vu au paragraphe 1.3.3 du chapitre 1, les EB_{DCC} sont considérés comme des EB indépendants. RSW peut par exemple générer un jeu de coupes où $EB_{DCC;1,2}$ et $EB_{DCC;2,3}$ sont présents dans la même coupe, au lieu de ne considérer que $EB_{DCC;tous}$ comme EB modélisant la défaillance simultanée pour causes communes des matériels 1, 2 et 3. De même, il peut par exemple considérer que

$EB_{DCC;1,2} \cap EB_{DCC;3,4} \neq \emptyset$. Toutefois, si on néglige ou si on supprime ces coupes, on peut tout de même appliquer la formule suivante si on accepte une approximation du risque par un développement de Poincaré à l'ordre 1 (hypothèse des événements rares). Sous cette hypothèse, on a toujours :

$$\begin{aligned} R = \quad & a_{int,i} \cdot (1-\beta) \cdot Q_{tot} + \sum_{j=1, i\neq j}^{m} a_{DCC;i,j} \cdot \frac{\beta \cdot (1-\gamma) \cdot Q_{tot}}{k_2} \\ & + \sum_{i\neq j, i\neq k, j\neq k} a_{DCC;i,j,k} \cdot \frac{\beta \cdot \gamma (1-\delta) \cdot Q_{tot}}{k_3} + a_{DCC,tous} \cdot \beta \cdot \gamma \cdot \delta \cdot Q_{tot} + b_{DCC;pas\ i} + b_i \end{aligned}$$

Cette expression est justifiée par le fait que la structure de l'arbre de défaillances modélisant la défaillance d'un EB appartenant à un groupe DCC (c.f. figure 1.6) permet de considérer qu'aucune coupe ne contient plus d'un EB_{DCC} impliquant l'occurrence de i et ce, quel que soit i. Pour plus d'informations, on pourra se reporter à [86]. Puisque RSW ne considère pas les événements incompatibles, il ne calculera pas directement le FAR d'un type d'événements associé à une cause mais une valeur qu'on appellera FAR_{RSW}, en considérant les événements DCC comme indépendants. On trouve alors que (c.f. [89]) :

$$\begin{aligned} FAR\left(EB_{int,i}\right) = \quad & FAR_{RSW}\left(EB_{int,i}\right) - \sum_{j\neq l} FDR_{RSW}\left(EB_{DCC;j,l}\right) \\ & - \sum_{j\neq l, j\neq k, l\neq k} FDR_{RSW}\left(EB_{DCC;j,l,k}\right) - FDR\left(EB_{DCC;tous}\right) \end{aligned}$$

$$\begin{aligned} FAR\left(EB_{DCC,\bullet}\right) = \quad & \left(\frac{1}{Q_{tot} \cdot \beta} - 1\right) \cdot \begin{pmatrix} \sum_{j=1, i\neq j}^{m} FDR_{RSW}\left(EB_{DCC;i,j}\right) \\ + \sum_{i\neq j, i\neq k, j\neq k} FDR_{RSW}\left(EB_{DCC;i,j,k}\right) \\ + FDR_{RSW}\left(EB_{DCC,tous}\right) \end{pmatrix} \\ & - FDR\left(EB_{int,i}\right) - \sum_{i\notin EB_{DCC;pas\ i}} FDR\left(EB_{DCC;pas\ i}\right) \end{aligned}$$

$$\begin{aligned} FAR\left(EB_i\right) = \quad & \left(\frac{1}{Q_{tot}} - 1\right) \cdot \begin{pmatrix} \sum_{j=1, i\neq j}^{m} FDR_{RSW}\left(EB_{DCC;i,j}\right) \\ + \sum_{i\neq j, i\neq k, j\neq k} FDR_{RSW}\left(EB_{DCC;i,j,k}\right) \\ + FDR_{RSW}\left(EB_{DCC,tous}\right) + FDR_{RSW}\left(EB_{int,i}\right) \end{pmatrix} \\ & - \sum_{i\notin EB_{DCC;pas\ i}} FDR\left(EB_{DCC;pas\ i}\right) \end{aligned}$$

2.3 *Facteurs d'importance d'un composant, d'un groupe de composants, d'une configuration*

En général, les facteurs d'importance sont calculés pour chaque événement de base, c'est-à-dire pour chaque mode de défaillance de chaque composant. De nouveaux facteurs d'importance ainsi que l'extension des facteurs d'importance existants ont été envisagés pour répondre à de nouveaux besoins. En effet, comme le rappelle Vesely dans [91], il n'est pas aisé d'établir le lien entre les facteurs d'importance de chaque EB et le facteur d'importance d'un ensemble d'événements. En général, on ne peut pas l'exprimer au moyen d'additions ou de multiplications des facteurs d'importance calculés au niveau des EB.

Importance d'un composant

La défaillance d'un matériel i n'est pas modélisée au moyen d'un seul EB mais à partir de plusieurs EB modélisant chacun un mode de défaillance de ce matériel. Ainsi, la défaillance

d'une vanne sera modélisée par deux EB, l'un modélisant le refus de fermeture et l'autre le refus d'ouverture.

De nombreuses références telles que [88, 89, 42] proposent d'exprimer l'importance d'un composant en fonction de l'importance de ses différents modes de défaillance. Pour ce faire, ces articles reposent sur l'hypothèse que les modes de défaillance d'un composant sont mutuellement exclusifs. Cette hypothèse est raisonnable. En effet, des événements comme "blocage ouvert de la vanne i" et "blocage fermé de la vanne i" ne peuvent pas se produire ensemble.

Sous cette hypothèse, on peut dire que pour le matériel m_i :

$$R = \sum_{j=1}^{k} a_{m_i,j} \cdot P\left(EB_{m_i,j}\right) + b_{m_i}$$

avec :

$EB_{m_i,j}$	un EB modélisant un mode de défaillance spécifique du matériel m_i
$a_{m_i,j}$	la valeur $P\left(CI/EB_{m_i,j}\right) - P\left(CI/\overline{EB_{m_i,j}}\right)$
k	le nombre de modes de défaillance de m_i
b_{m_i}	la valeur de $P\left(CI/\overline{EB_{m_i,j}}\right)$

On voit alors que le FAR d'un composant, par exemple, est égal à la somme des FAR de ses différents modes de défaillance :

$$FAR\left(m_i\right) = \sum_{j=1}^{k} FAR\left(EB_{m_i,j}\right)$$

Importance d'une configuration

Il est possible de calculer l'importance d'une "*configuration spécifique*". Une configuration spécifique doit être comprise comme la connaissance de l'état (réalisé ou non) de plusieurs EB. Vaurio propose dans [88] une mesure d'importance qu'il appelle "*Risk Gain (RG)*" et qui mesure le facteur d'accroissement de risque quand une configuration spécifique est connue.

Cette mesure d'importance nécessite de définir une configuration élémentaire contenant la combinaison simultanée d'événements dont l'occurrence ou la non-occurrence est certaine. On notera ces configurations CE_i (pour Configuration Élémentaire). RG est alors défini comme :

$$RG\left(CE_i\right) = \frac{P\left(CI/CE_i\right)}{P\left(CI\right)}$$

Si plusieurs configurations peuvent être envisagées, Vaurio propose de considérer des "*configurations générales*" qu'il définit comme un ensemble de configurations élémentaires CE_i auxquelles on associe une probabilité d'occurrence p_{CE_i}. Pour déterminer l'importance de ces "*configurations générales*", Vaurio propose d'utiliser une moyenne pondérée qui, pour une "*configuration générale*", définit RG comme :

$$RG\left(\underline{CE}, \underline{p}_{CE}\right) = \frac{\sum\limits_{i=1}^{N} p_{CE,i} \cdot P\left(CI/CE_i\right)}{\left(\sum\limits_{i=1}^{N} p_{CE,i}\right) \cdot P\left(CI\right)}$$

avec :

$\underline{CE}$	l'ensemble des configurations élémentaires de la configuration générale
$\underline{p}_{CE}$	le vecteur des probabilités de ces configurations élémentaires
N	le nombre de configurations élémentaires

Importance d'un système

Le mode de calcul de l'importance d'un système n'est pas clairement défini, tout comme la définition même de ce qu'est un système. En supposant qu'un système désigne l'ensemble des composants remplissant une fonction, certains considèrent qu'il faut calculer le risque sachant

que tous les matériels du système sont défaillants (cf. [41] ou [20] par exemple). Ainsi, Cheok [20] considère le risque sachant que tous les EB modélisant un mode de défaillance d'un des matériels du système sont certains. D'autres, comme Dutuit et Rauzy dans [36], proposent de calculer l'importance d'un événement correspondant à la défaillance d'un système exprimé au moyen d'une fonction de structure $\phi_{syst.\ i}(\underline{e})$ en estimant la probabilité $P(\Phi(\underline{e}) = \phi_{syst.\ i}(\underline{e}) = 1)$.

3 Applications actuelles et potentielles des facteurs d'importance

3.1 Application actuelle des facteurs d'importance

Lorsque l'on veut optimiser l'exploitation d'une centrale, une conception à l'étude, etc., il faut pouvoir s'orienter, par exemple, vers des matériels pour lesquels un gain en termes de risque ou de coûts d'exploitation est possible. C'est pour aider à cette orientation que les facteurs d'importance ont été employés.

Les facteurs d'importance sont des outils d'aide à la décision relativement polyvalents, ils interviennent donc dans de nombreuses applications. Des exemples d'application variés peuvent être cités, tels que l'aide à la (re-)conception, l'optimisation de la maintenance, la gestion de configuration, la définition des composants devant faire l'objet d'assurance qualité ou encore l'optimisation des périodicités de test. Pour illustrer ce à quoi peuvent servir et comment peuvent être utilisés les facteurs d'importance, l'exemple de l'optimisation de la maintenance par la fiabilité est exposé dans cette section.

Exemple de l'Optimisation de la Maintenance par la Fiabilité (OMF)

L'application la plus courante des facteurs d'importance est la redéfinition des politiques de maintenance et de test. Cette démarche, mise en œuvre aussi bien aux États-Unis [42, 94, 98] qu'en Espagne [64] ou en France [29, 27], repose sur la redéfinition des politiques de maintenance de chaque composant en fonction de son importance vis-à-vis du risque. Le but est de diminuer la maintenance des matériels qui, avant modification, sont peu importants et d'augmenter l'efficacité de la maintenance des matériels importants pour le risque avant modification.

En résumé, la démarche est la suivante :

A partir de modèles EPS dont on a vérifié la complétude, on calcule le FAR et le FDR de chaque matériel. On connaît alors l'importance relativement au risque de chaque matériel avant la modification des politiques de maintenance. Ensuite, chaque matériel est classé en fonction de la valeur de son FAR et de son FDR. Suite à ce classement, les propositions suivantes de modifications du programme de maintenance sont envisagées :

- la maintenance préventive des matériels dont le FDR est très élevé doit être améliorée dans la mesure du possible ou, a minima, maintenue,
- les matériels ayant un FAR très élevé doivent faire l'objet d'une surveillance et leur maintenance préventive doit être maintenue ou légèrement relâchée,
- les matériels dont le FAR et le FDR sont faibles peuvent faire l'objet d'une maintenance uniquement corrective.

Ces propositions de modification sont alors revues par un panel d'experts qui ont pour tâche de vérifier que tous les composants considérés comme non importants (au vu des indicateurs de l'OMF) le sont réellement. En effet, comme les EPS n'ont qu'un domaine de couverture limité[11],

[11] Les EPS utilisées par EDF pour appliquer la méthode OMF sont des EPS de niveau I ne considérant que des événements internes. L'importance des digues protégeant d'une intrusion d'eau en cas d'ouragan (événement externe à la centrale) ou de systèmes utilisés une fois la fusion du cœur avérée (non pris en compte dans une EPS de niveau I) est fortement sous-estimée.

un événement que les experts reconnaissent comme important pour le risque ou la sûreté peut avoir un faible FAR et un faible FDR. Il peut même ne pas être modélisé. Ensuite, on estime le coût lié à l'indisponibilité et les coûts de maintenance corrective des matériels dont on veut relâcher la maintenance. S'ils sont inférieurs au coût avant modification de la maintenance et que le panel d'experts est d'accord, la maintenance de ces matériels peut être modifiée.

3.2 Développement possible de l'utilisation des mesures d'importance : l'aide à la conception

Conception et EPS

Lors de la conception de la majorité des centrales aujourd'hui en exploitation, les EPS n'existaient pas encore. Les démarches de conception qui ont été élaborées ne reposaient pas du tout sur ces outils. Aujourd'hui, les EPS sont des outils reconnus et largement utilisés, qui doivent être intégrés dans le processus de conception des nouvelles centrales. Ainsi, l'AIEA précise dans [5] que "*pour les futures centrales, une approche probabiliste sera menée de manière conjointe à l'approche déterministe*".

En conséquence, elle propose une démarche de conception reposant sur le schéma de la figure 1.10.

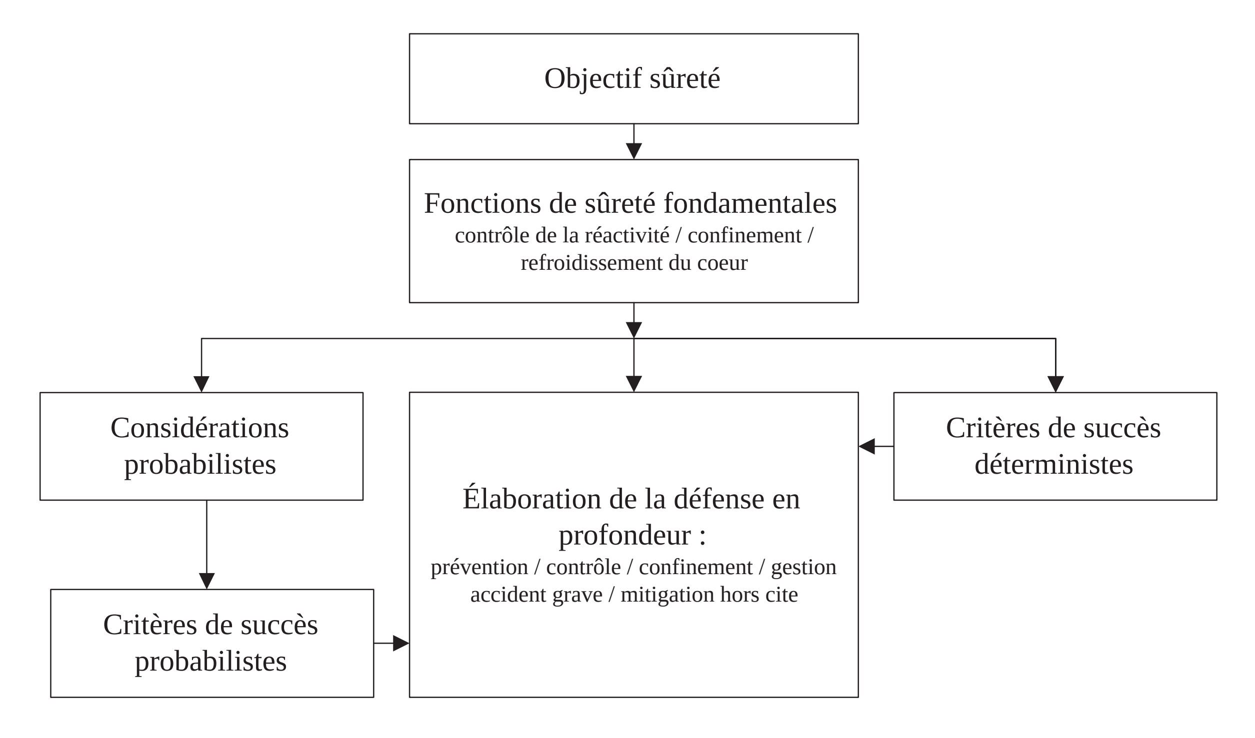


Fig. 1.10 – *Démarche de conception préconisée par l'AIEA*

En France aussi, les EPS sont perçues comme des outils pertinents pour l'aide à la conception. Ainsi, le Groupe Consultatif Français de Sûreté précise dans [55] que "*les EPS seront développées et enrichies par étapes successives tout au long du cycle de développement des réacteurs futurs*" tout en soulignant que "*les EPS sont des outils nécessaires mais pas suffisants pour juger du niveau de sûreté. Elles font partie de la démarche de sûreté globale et itérative, où elles sont à la fois une source de questionnement (par exemple, identification de situations physiques à étudier) et un outil de validation des options retenues*".

Définition des lignes de défense

Quel que soit le type de technologie employé et quelle que soit la démarche de conception choisie, les enjeux sont toujours, pour un coût de construction et d'exploitation donné et une disponibilité de la centrale donnée, de concevoir la centrale la plus sûre possible.

Pour atteindre cet objectif, des lignes de défense sont créées pour prévenir ou mitiger les conséquences d'un événement perturbateur. Afin de garantir un niveau de risque acceptable, plusieurs lignes de défense indépendantes doivent s'interposer entre un événement perturbateur et l'atteinte de conséquences inacceptables.

Pour pouvoir travailler sur la conception et la répartition des lignes de défense, il faut au préalable les définir. De nombreux auteurs se sont attachés à préciser et classifier des termes tels que "*barrière de sûreté*", "*fonction de sûreté*", "*ligne de défense*", etc [50, 60, 97, 61, 57, 34, 33].

Pour clarifier ces termes, dans ce mémoire, on utilise la définition proposée dans [80]. Une barrière de sûreté est définie comme "*un moyen, physique ou non, de prévenir, contrôler ou mitiger un événement non-désiré ou un accident*", une fonction barrière est "*une fonction prévue pour prévenir, contrôler ou mitiger un événement non-désiré ou un accident*" et enfin un système barrière est "*un système qui a été conçu et qui est mis en œuvre pour supporter une ou plusieurs fonctions barrières* ".

Par la suite, le terme de "fonction de sûreté" sera réservé à la désignation des trois fonctions de sûreté : maîtriser la réactivité, refroidir le combustible et confiner les produits radioactifs [39]. Pour de nouveaux types de centrale, on peut imaginer que ces fonctions soient légèrement différentes, mais dans tous les cas le terme "fonction de sûreté" sera réservé à la désignation de quelques fonctions essentielles dont la perte entraîne l'atteinte de conséquences inacceptables.

Pour mémoire, le terme "barrière physique", déjà mentionné en introduction, désigne les obstacles physiques conçus pour empêcher la dispersion des produits radioactifs.

Enjeux de la conception

Pour que le coût de construction et d'exploitation ne soit pas trop élevé, il faut que les lignes de défense s'interposant entre initiateur et accident garantissent un niveau de risque acceptable mais ne soient pas trop nombreuses. L'un des objectifs de la conception d'une centrale est donc de s'assurer de la bonne couverture de tous les risques et de la robustesse de l'installation face à des événements perturbateurs sans pour autant se sur-protéger contre certains risques.

Pour atteindre un niveau de risque acceptable à moindre coût, les lignes de défense doivent être indépendantes et concentriques.

Ainsi, pour l'AIEA, l'indépendance des lignes de défense est un objectif prioritaire. En effet, dans [6], on peut lire que "*les concepteurs des systèmes de sûreté doivent s'assurer de toutes les manières possibles que les différents systèmes de sauvegarde protégeant les barrières physiques sont fonctionnellement indépendants dans les conditions d'un accident*".

De même, dans [50], Fleming souligne qu'un objectif important, lors de la conception des lignes de défense, est d'en garantir l'indépendance et la concentricité. Ainsi, chaque ligne de défense doit être à même de diminuer l'impact d'un initiateur et/ou de la défaillance de n'importe quelle autre ligne de défense.

En d'autres termes, chaque ligne de défense doit être la plus indépendante possible des autres, la plus robuste possible et la plus polyvalente possible. Ainsi, si des lignes de défense très polyvalentes sont développées (par exemple, des lignes de défense fonctionnant pour tout initiateur, quelles que soient les conditions physiques), elles n'ont pas besoin d'être nombreuses. On contribue alors à la simplicité de l'installation.

Si on fait l'analogie avec un château fort, on préférera une répartition des lignes de défense concentrique à une répartition non concentrique :

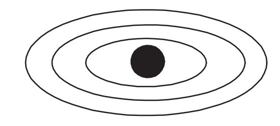


Fig. 1.11 – *Lignes de défenses concentriques*

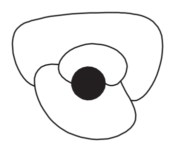


Fig. 1.12 – *Lignes de défenses non concentriques*

En effet, dans le premier exemple, d'où que viennent les "assaillants", ils doivent franchir les trois lignes de défense. Dans le second cas en revanche, ils peuvent choisir une trajectoire telle qu'ils n'aient à traverser qu'une seule barrière. Ainsi, une centrale nucléaire idéale ne comporterait que quelques lignes de défense qui seraient utilisées pour parer à n'importe quel initiateur. Dans ce cas idéal, chaque arbre d'événements aurait pour structure celle de la figure 1.13, et ce, quel que soit i. On a alors bien des lignes de défense concentriques : chaque ligne de défense arrête l'accident quel que soit l'initiateur et la défaillance de l'une d'elle ne court-circuite pas la suivante.

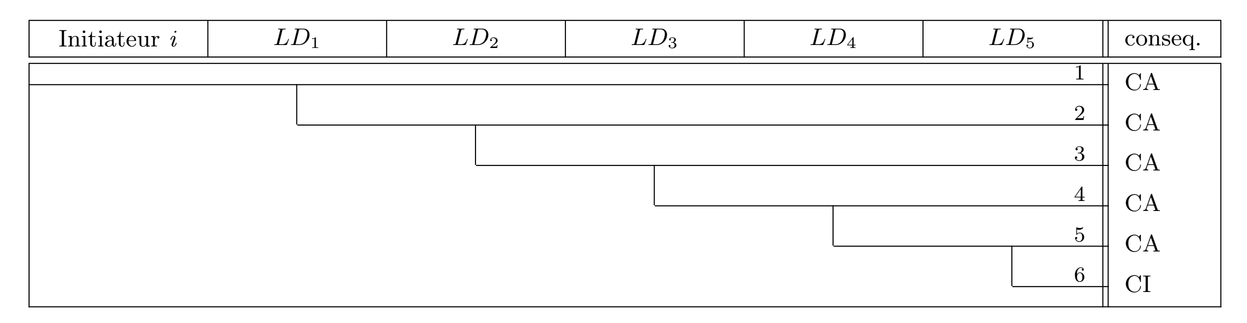


Fig. 1.13 – *Arbre d'événements idéal*

L'utilisation de démarches de type EPS pour l'aide à la conception semblent très prometteuse mais de telles démarches n'ont pas encore été mises en œuvre. Elles restent à élaborer.

4 Limites des démarches de prise de décision basées sur les facteurs d'importance

4.1 Limites théoriques

Les différentes applications des facteurs d'importance sont toutes sujettes à des limitations d'un point de vue théorique. Ces limitations peuvent s'exposer suivant deux axes. Tout d'abord, l'importance d'un événement, exprimée au moyen de ses facteurs d'importance, est relative au contexte dans lequel on considère cet événement. De plus, on n'a aucune visibilité quant au risque résultant d'une décision prise au moyen de facteurs d'importance.

4.1.1 L'importance d'un événement n'existe pas de manière absolue

Des indicateurs relatifs à la valeur du risque de référence

Exceptés le facteur DIM et l'indicateur de Birnbaum, tous les autres facteurs d'importance font intervenir la valeur de R. De ce fait, si on prend une décision en comparant la valeur d'un facteur d'importance à un seuil, cette décision dépendra évidemment de l'importance de l'événement étudié mais aussi du risque de référence de la centrale étudiée.
Par exemple, le FAR d'un événement i exprime l'accroissement de risque $(R_{1,i} - R)$ consécutif à

l'occurrence devenue certaine de EB_i divisé par le risque. Ainsi, pour un même accroissement de risque, plus R est faible, plus le FAR sera élevé, moins l'occurrence de EB_i paraîtra acceptable. Pourtant, on pourrait au contraire penser que cet accroissement de risque peut être acceptable pour une centrale sûre et non pas pour une centrale déjà peu sûre.

L'importance d'un événement dépend des autres

Quel que soit l'événement considéré et quel que soit le facteur d'importance utilisé, on ne connaît l'importance de l'événement que relativement aux autres composants. L'importance d'un événement pour le risque ou la sûreté n'est pas une propriété intrinsèque.

En effet, comme on l'a vu au paragraphe précédent, la plupart des facteurs d'importance incluent le risque de référence dans leur formule. Puisqu'ils dépendent du risque, ils dépendent de la fonction de structure et de la probabilité d'occurrence de tous les autres composants. De plus, un composant i peut n'être important, ni pour le risque, ni pour la sûreté, s'il n'intervient que dans des coupes composées d'autres événements ayant une très faible probabilité d'occurrence. Si cette probabilité augmente, l'importance de i augmentera d'autant. De même, si l'occurrence de certains événements est certaine, l'importance du composant étudié peut croître rapidement. L'état de la tranche à l'instant où l'on veut considérer l'importance d'un événement a un impact significatif sur l'estimation de cette importance via les facteurs d'importance. Les facteurs d'importance tels qu'ils sont décrits dans la section 2.1.3 du chapitre 1 ne nous donnent que l'importance moyenne sur une année d'un événement [93].

Des indicateurs relatifs à la nature du risque considéré

Comme le rappelle Vesely dans [91], l'importance d'un événement dépend de la nature du risque considéré. Par exemple, si on se place dans le cadre d'une EPS de niveau 1, les matériels ne visant qu'à confiner dans le bâtiment réacteur les substances radioactives ont une importance nulle. En revanche, si on considère que CI correspond à l'événement "rejet de substances radioactives dans l'atmosphère" comme c'est le cas dans les EPS de niveau 2, ces matériels peuvent devenir primordiaux.

Conclusion sur l'importance relative des événements

Quel que soit l'événement de base considéré, son importance dépend donc du risque considéré, de la fonction de structure $\Phi\left(\underline{e}\right)$ (est-il dans des coupes d'ordre élevé ?) et de la probabilité d'occurrence $\underline{p}$ des autres EB.

Comme le dit Vesely dans [92], les facteurs d'importance ne permettent que de retrouver "*les événements dont l'importance est anormalement élevée*" pour une conception et une fiabilité des matériels données. Dans un système bien conçu où la défaillance de chaque matériel a un impact identique sur le risque, les facteurs d'importance nous indiqueraient qu'aucun d'eux n'est important alors que tous le sont.

4.1.2 Une estimation difficile de l'impact des décisions basées sur les facteurs d'importance

Si les facteurs d'importance permettent, pour une conception donnée et une probabilité d'occurrence de chaque EB donnée, de connaître les composants dont l'importance est élevée, il est relativement difficile d'estimer les impacts sur le risque d'une décision basée sur les facteurs d'importance au moyen de ces mêmes facteurs d'importance.

Une difficile estimation du risque après modification

Pour estimer le risque après une modification impactant un EB_i, on peut utiliser le FDR qui nous donne l'accroissement relatif de risque lorsque sa probabilité d'occurrence est doublée ou le FAR qui donne l'accroissement relatif de risque lorsque cet événement devient certain. On a

alors un majorant indiscutable du risque quelles que soient les modifications décidées impactant cet EB. Toutefois, si ce raisonnement est valable à l'échelle d'un composant, il est plus difficile à étendre lorsque l'on prend des décisions impactant plusieurs composants [91]. On pourrait alors estimer le risque sachant l'indisponibilité simultanée de l'ensemble des composants impactés mais, outre le fait que cette variation de risque, bien que majorante, est irréaliste, il n'est pas aisé (excepté pour le facteur DIM) de connaître l'importance d'un groupe à partir de celle de chacun de ses événements de base [92].

Il apparaît donc difficile d'avoir une idée de l'impact sur le risque d'une décision basée sur les facteurs d'importance.

Exemple : Dans le cadre d'une démarche OMF, on sélectionne tous les matériels qui, pris individuellement, sont peu importants pour le risque ou la défense en profondeur. Ils ne font ensuite plus l'objet que d'une maintenance corrective qui peut entraîner une défiabilisation de chacun d'eux. Mais, sans précaution, rien ne dit que cet ensemble de composants, une fois défiabilisés, n'affaiblira pas significativement une ou plusieurs lignes de défense. Si on prend l'exemple d'une coupe $EB_1 \cap EB_2 \cap EB_3$ dont chaque événement de base a une probabilité d'occurrence de 10^{-5}, la probabilité de cette coupe est de 10^{-15} et, même lorsqu'un de ces événements est certain, sa probabilité reste faible : 10^{-10}. Si les événements de cette coupe deviennent plus probables, par exemple 10^{-2}, la probabilité de cette coupe devient importante : 10^{-6}. En ne défiabilisant que des EB qui, lorsqu'ils sont pris individuellement, sont peu importants, on a donc contribué à transformer une coupe non-significative en l'une des coupes contribuant le plus à la valeur du risque de référence.

Le risque n'est pas le seul critère

Fonder une décision uniquement sur des indicateurs de risque occulte son impact sur les coûts de maintenance et sur les coûts d'indisponibilité. Ainsi, si on prend l'exemple d'une "optimisation" de la maintenance en ne considérant que l'impact sur le risque de chaque événement, il peut être plus coûteux de ne faire que de la maintenance corrective. En effet, lorsque l'on veut ne mettre en place que de la maintenance corrective, les coûts d'indisponibilité peuvent être prohibitifs. Si on prend l'exemple de la turbine, ce composant ne joue quasiment aucun rôle dans la sûreté de la centrale. Pour autant, il apparaît aberrant de ne pas faire de maintenance préventive sur ce composant au vu de son importance pour la disponibilité de la centrale.

Une analyse de risque doit souvent être couplée, comme c'est le cas pour l'OMF, à une analyse économique pour permettre des prises de décision optimisées pour la sûreté et pour les coûts d'exploitation.

4.2 Limites dues aux incertitudes sur les mesures d'importance

Les limites de la prise de décision basée sur les facteurs d'importance dépendent de la définition théorique de ces indicateurs (caractère relatif, non-méconnaissance de l'impact sur le risque, etc.). Elles dépendent aussi des incertitudes qui affectent les facteurs d'importance. En effet, si les incertitudes sur ces facteurs sont trop importantes et si elles ne sont pas prises en compte, certains événements importants pour le risque ou la sûreté risquent de ne pas être détectés et on prendra des décisions trop optimistes. Il faut donc réduire et, a minima, caractériser ces incertitudes pour bien orienter les prises de décision qui découlent des facteurs d'importance.

4.2.1 Incertitudes liées à la taille des modèles EPS

Comme on l'a vu dans la section 1.2.5 du chapitre 1, les modèles EPS sont de gros modèles et le jeu de coupes doit être tronqué pour respecter les limites physiques des ordinateurs qui servent à les générer. Si le choix du seuil de troncature est pertinent, le risque de référence est très peu sous-estimé (Δ_{TR} petit).

La question est de savoir quel est l'impact de la troncation sur le calcul des facteurs d'importance. Comme on l'a vu dans la section 2.1.3 du chapitre 1, les facteurs d'importance courants reposent sur le calcul de R, $R_{1,i}$ et $R_{0,i}$. Il faut donc voir quel impact a la troncation sur ces valeurs en fonction du mode de calcul de ces valeurs. Le calcul de $R_{1,i}$ et de $R_{0,i}$ peut se faire de deux façons :

- en quantifiant ces valeurs une à une à partir de modèles dédiés : on parlera alors d'une approche manuelle (on est obligé de créer les modèles dédiés "à la main"),
- en déduisant ces valeurs de l'étude du jeu de coupes de référence : on parlera alors d'un calcul automatique basé sur un jeu de coupes.

Dans cette section, on étudiera donc l'impact de la troncation sur les mesures d'importance en fonction de leur mode de calcul.

Calcul "manuel" de $R_{1,i}$ et $R_{0,i}$

Mode de calcul : $R_{1,i}$ (respectivement $R_{0,i}$) est calculé en générant à partir du modèle le jeu de coupes correspondant à la situation où l'occurrence de l'EB_i est certaine (respectivement impossible). Pour ce faire, dans le modèle EPS, on précise que l'événement EB_i est "VRAI" (respectivement "FAUX"), puis on relance le calcul du risque pour obtenir $R_{1,i}$ (respectivement $R_{0,i}$) en utilisant le même seuil de troncature que pour le risque de référence, S_p.

Incertitude lors d'un calcul manuel : Les logiciels supports des EPS fournissent un majorant de l'incertitude sur $R_{1,i}$, appelé $\Delta_{TRM;1,i}$ (le grand M en indice précise qu'il s'agit d'un majorant de la vraie erreur $\Delta_{TR;1,i}$), et sur $R_{0,i}$, appelé $\Delta_{TRM;0,i}$. Ces deux majorants sont en général du même ordre que Δ_{TRM}, le majorant de Δ_{TR} fourni par les logiciels supports. En effet, on utilise, pour générer les coupes correspondant à $R_{1,i}$ (respectivement $R_{0,i}$), le même processus de troncature que lorsqu'on calcule le risque de référence. On peut donc s'attendre à obtenir la même incertitude liée à la troncation du jeu de coupes.

Intérêt de ce mode de calcul : Avec ce mode de calcul "manuel", on dispose d'un majorant de l'incertitude sur $R_{1,i}$ et $R_{0,i}$ et il est en général acceptable. Toutefois, ce mode de calcul nécessite une modification manuelle du modèle pour chaque valeur de i et une re-génération d'un jeu de coupes. Le temps nécessaire à cette dernière étape peut se compter en heures suivant la taille du modèle. Le temps de calcul de $R_{1,i}$ et $R_{0,i}$, pour les milliers d'EB présents dans un modèle EPS, se compte donc en semaines, voire en mois. Chaque modification du modèle implique un changement de la valeur de R et donc de la valeur de tous les facteurs d'importance. A chaque modification du modèle, il faudrait donc recalculer tous les facteurs d'importance, ce qui nécessiterait plusieurs semaines de travail pour chaque modification. Ce coût est trop important pour pouvoir être consenti à long terme. Une approche plus automatique, plus "industrielle", doit être mise en œuvre.

Calcul automatique de $R_{1,i}$ et $R_{0,i}$ à partir d'un jeu de coupes

Mode de calcul : Le risque de référence R est calculé, les coupes de référence dont la probabilité d'occurrence est supérieures à S_p sont générées avec un majorant de l'incertitude due à la troncation sur R qui est Δ_{TR}. $R_{1,i}$ et $R_{0,i}$ sont alors calculés à partir de ce jeu de coupes. Pour ce faire, lorsqu'on calcule $R_{1,i}$:

- on recalcule la probabilité de chaque coupe de référence $CM_{ref.,j}$ contenant EB_i en multi-

pliant son ancienne probabilité par $\frac{1}{P(EB_i)}$ et on supprime l'événement EB_i de cette coupe,

- pour toutes les coupes ne contenant pas EB_i, on vérifie qu'elles restent minimales. Si ce n'est pas le cas, on les extrait du jeu de coupes. En effet, la coupe de référence $EB_2 \cap EB_3 \cap EB_4$ devient non minimale s'il existe une autre coupe de référence $EB_i \cap EB_2 \cap EB_3$ quand EB_i est considéré comme certain.

On obtient alors un jeu de coupes, issu du jeu de coupes de référence, qui correspond à $R_{1,i}$.

Pour calculer $R_{0,i}$, il suffit de supprimer, parmi les coupes de référence, celles qui contiennent EB_i. On obtient alors un jeu de coupes, issu du jeu de coupes de référence, qui correspond à $R_{0,i}$.

Incertitude liée la troncation du jeu de coupes de référence sur les facteurs d'importance calculés avec la méthode automatique : Les coupes de référence contenant EB_i forment un sous-ensemble des coupes de référence. De même, les coupes contenant EB_i supprimées lors de la troncation forment un sous-ensemble des coupes de référence tronquées. La probabilité d'occurrence d'une des coupes supprimées contenant EB_i est donc inférieure ou égale à Δ_{TR}. De même, la probabilité d'occurrence d'une des coupes supprimées ne contenant pas EB_i est donc inférieure ou égale à Δ_{TR}.

L'erreur sur $R_{0,i}$ due à la troncation des coupes de référence correspond à la probabilité des coupes supprimées lors de la troncation et ne contenant pas EB_i. Dans le pire des cas, toutes les coupes supprimées ne contiennent pas EB_i. On a donc $\Delta_{TR;0,i} \leq \Delta_{TR}$ [41] lorsque $R_{0,i}$ est calculé à partir des coupes de référence.

Pour connaître la sous-estimation de $R_{1,i}$ due à la troncation du jeu de coupes de référence, on s'intéresse aux coupes de référence supprimées contenant EB_i. La sous-estimation de $R_{1,i}$ correspond donc à la probabilité de ces coupes divisée par $P(EB_i)$ (car EB_i est certain). Dans le pire des cas, toutes les coupes tronquées contiennent EB_i. Dans ce cas, le seul majorant qu'on puisse considérer est $\Delta_{TRM;1,i} \leq \frac{\Delta_{TRM}}{P(EB_i)}$ [41]. Pour un EB dont la probabilité d'occurrence est faible, ce majorant peut être très élevé.

Puisque l'EB étudié peut être présent dans toutes les coupes tronquées, il faut donc avoir un majorant de l'erreur due à la troncation du jeu de coupes (Δ_{TRM}) de référence très petit pour pouvoir garantir un calcul précis des différents facteurs d'importance nécessitant le calcul de $R_{1,i}$.

Exemple de majorant de l'erreur : Supposons que le jeu de coupes de référence ait été généré avec un seuil de troncature S_p ayant pour valeur 10^{-12}. On obtient alors un risque de référence R valant $5 \cdot 10^{-5}$ et un majorant de l'incertitude due à la troncation Δ_{TRM} de $2,5 \cdot 10^{-6}$.

Quel que soit l'EB_i considéré et quelle que soit sa probabilité d'occurrence, l'erreur sur son FDR due à la troncation du jeu de coupes de référence sera alors majorée par :

$$\begin{aligned}
\Delta_{FDR} &\leq \frac{\Delta_{TRM}}{R} \\
&\leq \frac{2,5 \cdot 10^{-6}}{5 \cdot 10^{-5}} \\
&\leq 0,05
\end{aligned}$$

Pour un EB_i dont la probabilité d'occurrence est de 10^{-6}, l'erreur sur son FAR due à la

troncation du jeu de coupes de référence sera alors majorée par :

$$\begin{aligned} \Delta_{FAR(EB_i)} &\leq \frac{\Delta_{TRM}}{R \cdot P\left(EB_i\right)} \\ &\leq \frac{2,5 \cdot 10^{-6}}{5 \cdot 10^{-5} \cdot 10^{-6}} \\ &\leq 5 \cdot 10^{4}\,\mathbf{!\,!} \end{aligned}$$

Le majorant de l'erreur sur le FAR de l'EB_i apparaît énorme lorsque l'on sait que l'EPRI considère dans [42] que les FAR supérieurs à 1 caractérisent les EB significatifs pour la sûreté. On peut raisonnablement supposer que ce majorant est bien trop supérieur à la valeur réelle du FAR.

Un impact proportionnel à la probabilité de chaque EB
Lorsque $R_{1,i}$ est calculé pour EB_i à partir des coupes de référence (deuxième méthode), l'impact de la troncation du jeu de coupes sur la sous-estimation de $R_{1,i}$ est fonction de la probabilité d'occurrence de EB_i.

En effet, avec une troncation probabiliste des coupes de référence, quelle que soit la valeur du seuil S_p, les coupes les moins significatives pour le risque de référence sont supprimées. Lorsque l'on considère EB_i comme un événement certain, les coupes non significatives contenant cet EB voient leur probabilité d'occurrence multipliée par $\frac{1}{P\left(EB_i\right)}$. Pour être sûr de bien estimer $R_{1,i}$, il faut pouvoir garantir que les coupes considérées comme non significatives dans le cadre du risque de référence le sont toujours après multiplication de leur probabilité d'occurrence par ce facteur.

Exemple : Le jeu de coupes correspondant au risque de référence du modèle `900PREVD3` contient une coupe qui est :

$$-OR8_J \cap ASG001BABPR_DF \cap PTR017MN_24_IDCCA$$

Cette coupe a une probabilité d'occurrence de $9,334 \cdot 10^{-13}$. La probabilité d'occurrence de l'EB $ASG001BABPR_DF$ est de $8 \cdot 10^{-7}$. La probabilité de cette coupe quand cet EB est considéré comme certain est alors de $1,167 \cdot 10^{-6}$. Supposons que ce modèle ait été généré avec un seuil probabiliste S_p de 10^{-12}. Alors cette coupe est supprimée lors de la génération des coupes. Lors du calcul de $R_{1,ASG001BABPR_DF}$ à partir du jeu de coupes correspondant au risque de référence, on négligera donc une coupe de probabilité d'occurrence de $1,167 \cdot 10^{-6}$!

La figure 1.14 illustre bien le fait que pour un EB peu probable ($<10^{-5}$), il faut avoir un seuil de troncature très bas pour obtenir une valeur précise de $R_{1,i}$. Le cas est extrait du modèle EPR, mais des cas de ce type se trouvent dans les différents modèles.

On voit alors que, plus la probabilité d'occurrence d'un EB i sera faible, plus la valeur de $R_{1,i}$ calculée à partir de ces coupes de référence risquera d'être sous-estimée. Ainsi, pour un seuil S_p ayant une valeur fixée, la valeur de $R_{1,i}$ sera plus sous-estimée pour des EB ayant une faible probabilité d'occurrence que pour des EB relativement probables. Le classement des différents EB en fonction de leur importance peut être modifié suivant la valeur du seuil ayant servi à générer les coupes de référence dont l'estimation de ces importances est issue.

Exemple : La figure 1.15 présente les valeurs de $R_{1,i}$ calculées à partir des coupes de référence en fonction du seuil de troncation probabiliste utilisé pour générer ce jeu de coupes de référence. Les EB étudiés correspondent à des défaillances de tableau électrique, à des défaillances de vannes ou à des fuites.

Si on considère cette figure et qu'on considère l'importance des différents EB à partir de leur FAR (fonction de $R_{1,i}$ et de R uniquement), on voit que :

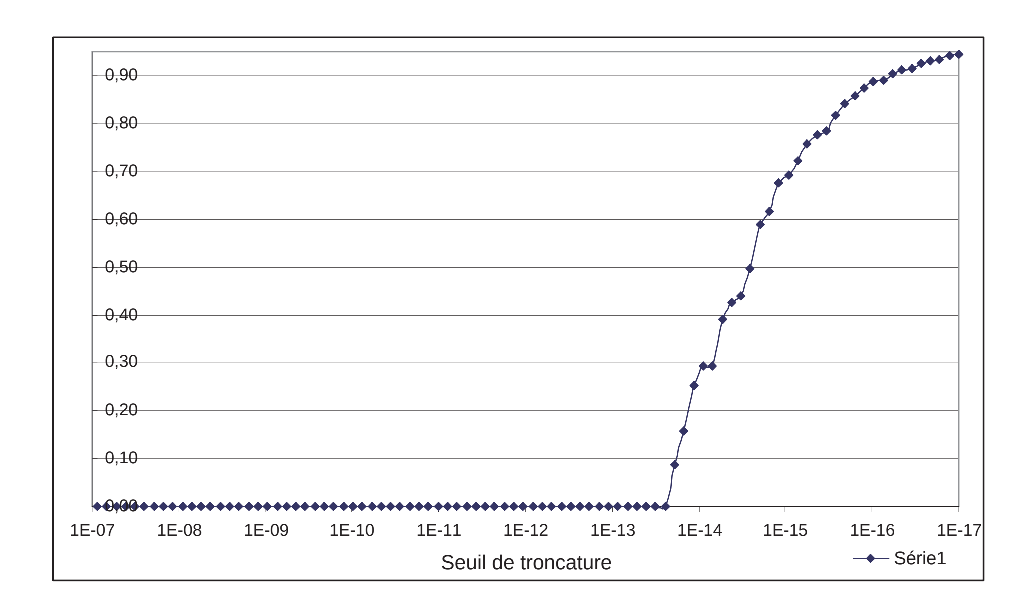


FIG. 1.14 – *Evolution de la valeur du FAR de l'EB RCV7115VBEEL (proba. d'occurrence 4,2E-7) en fonction du seuil de troncature probabiliste (S_p)*

- Pour un seuil de 10^{-11}, seuls deux EB sont importants. Ce sont EB_6 et EB_4. Tous les autres ont un FAR nul. Le classement par importance décroissante est EB_6 puis EB_4.
- Pour un seuil de 10^{-12}, trois EB sont importants. Ce sont EB_6, EB_5 et EB_4. Tous les autres ont un FAR nul. Le classement par importance décroissante est EB_6 puis EB_5 puis EB_4.
- Pour un seuil de 10^{-14}, ce sont toujours les trois mêmes EB qui sont importants mais leur classement est maintenant : EB_5 puis EB_6 puis EB_4.
- Enfin pour un seuil de 10^{-19}, tous les EB sont considérés comme importants et ceux qu'on considérait avant comme non-importants sont maintenant ceux qui ont la plus grande importance. Le classement est finalement : EB_2 puis EB_1 puis EB_3 puis EB_5 puis EB_6 puis EB_4.

La mésestimation de l'importance des EB 1, 3 et 5 pour des valeurs de seuil supérieures à 10^{-17} s'explique par le fait que leur probabilité d'occurrence est faible comparée à celle des EB 6 et 4.

Cet exemple illustre bien le fait que non seulement les valeurs des facteurs d'importance dépendent du seuil de troncature utilisé pour générer les coupes de référence dont ils sont issus, mais, de plus, l'erreur commise n'est pas uniforme sur tous les facteurs d'importance. En effet, si on classe les EB de cet exemple en fonction de leur FAR (qui dépend de $R_{1,i}$) le classement change en permanence en fonction du seuil. Il peut même totalement s'inverser entre deux valeurs, comme on peut le voir dans la figure 1.15.

Choix du seuil de troncature du jeu de coupes de référence utilisé pour le calcul des facteurs d'importance : La troncation du jeu de coupes de référence impacte surtout le calcul de $R_{1,i}$. On ne considère, dans ce paragraphe, que la gestion de son incertitude[12].

Il faut modifier le seuil de troncature utilisé pour générer les coupes correspondant au risque de référence si on veut s'en servir pour calculer les valeurs de $R_{1,i}$ pour différents EB (différentes valeurs de i). Ainsi, on doit s'attacher à trouver un seuil qui permette de garder à la fois les coupes significatives pour R et les coupes potentiellement significatives, c'est-à-dire les coupes

[12] L'incertitude sur $R_{0,i}$ due à la troncation du jeu de coupes de référence dont cette valeur est issue est toujours acceptable si l'incertitude sur R l'est.

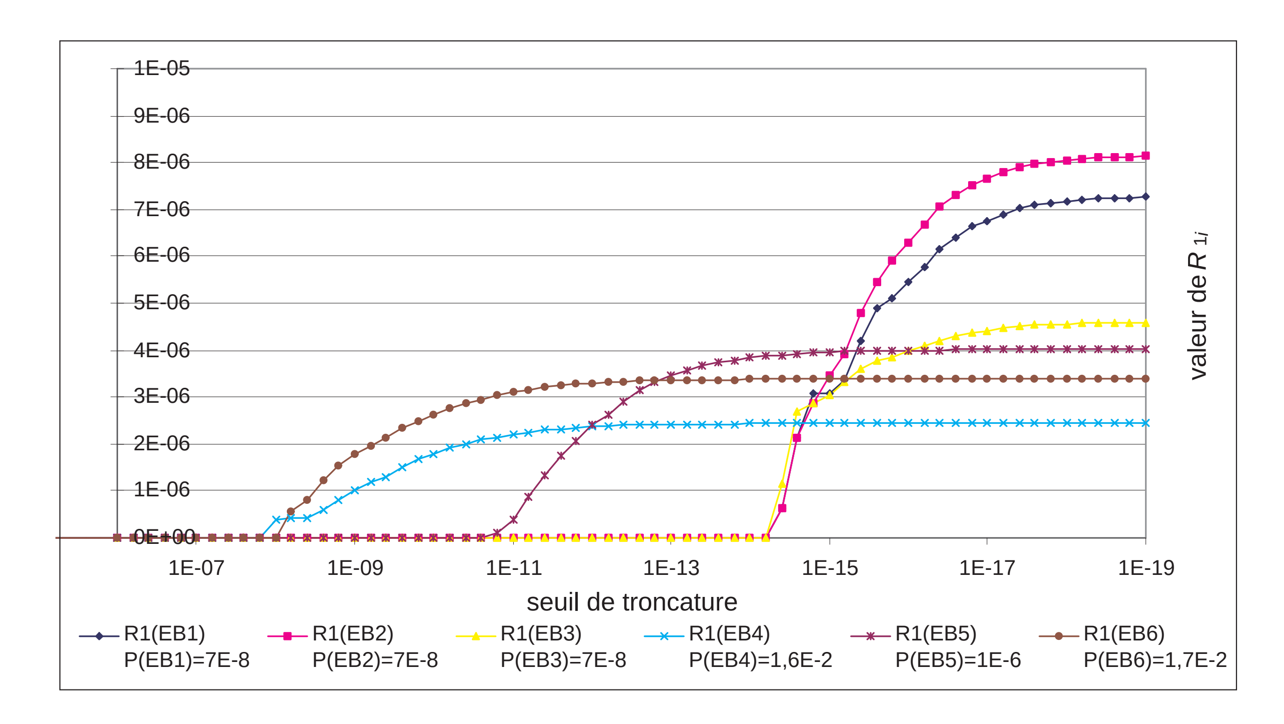


FIG. 1.15 – *Évolution de $R_{1,i}$ en fonction du seuil pour différents EB*

qui deviennent significatives lorsque l'un de leurs EB est considéré comme certain.

Baser le choix du seuil sur le majorant de l'erreur

Comme on l'a vu au paragraphe précédent, le majorant de $\Delta_{TR;1,i}$ dépend de Δ_{TR} qui dépend de S_p. Plus S_p est faible, plus Δ_{TR} est faible et plus l'incertitude sur $R_{1,i}$ due à la troncation du jeu de coupes de référence est acceptable. Il faut donc définir un processus de choix de la valeur de S_p pour que l'incertitude sur $R_{1,i}$ soit maîtrisée.

La solution la plus simple serait de descendre la valeur de S_p pas à pas jusqu'à ce que $\dfrac{\Delta_{TRM}}{\min\limits_{i\in[1,k]}[P(EB_i)]}$ devienne acceptable (avec de 1 à k les EB dont on veut connaître l'importance). Cette démarche n'est pas réalisable car Δ_{TRM} est souvent un majorant élevé (bien supérieur à l'erreur réelle Δ_{TR}) et l'erreur estimée reste très importante jusqu'à ce qu'on atteigne les limites de l'ordinateur utilisé pour générer les coupes supérieures à S_p. Une solution peut être d'affiner le majorant de Δ_{TR} dans les logiciels supports, comme le propose Jung dans [62].

Test de convergence pour déterminer le seuil de troncature

Čepin propose dans [19] une démarche alternative reposant sur la recherche itérative de la convergence de $R_{1,i}$ et de R. Le principe de cette approche est de supposer que :
- le risque est une fonction concave de S_p,
- R et $R_{1,i}$ convergent vers une valeur finie.

Cette approche, appliquée à notre cas, peut être résumée de la manière suivante :

1. La valeur du seuil de troncature S_p est diminuée pas à pas (S_{p_k} correspond à la valeur de S_p à la $k^{\text{ème}}$ itération). Quand l'augmentation de la valeur de $R_{1,i}$ entre $R_{1,i;S_{p_k}}$ calculé avec le seuil S_{p_k} et $R_{1,i;S_{p_{k+1}}}$ calculé avec le seuil $S_{p_{k+1}}$ devient négligeable, S_{p_k} est considéré comme acceptable pour le calcul de $R_{1,i}$.
2. La même démarche est effectuée pour le risque de référence. Quand l'augmentation de la valeur de R entre $R_{S_{p_j}}$ calculé avec le seuil S_{p_j} et $R_{S_{p_{j+1}}}$ calculé avec le seuil $S_{p_{j+1}}$ devient négligeable, S_{p_j} est considéré comme acceptable pour le calcul du risque de référence.

3. la plus petite valeur entre S_{p_k} et S_{p_j} est sélectionnée comme seuil de troncature acceptable pour le calcul des facteurs d'importance.

Cette approche semble bien adaptée au choix d'un seuil de troncature pour le calcul du risque de référence. En effet, même si l'hypothèse de concavité ne peut être démontrée de manière théorique, l'observation des modèles existants semble la valider, comme l'illustre la figure 1.16.

Elle est en revanche moins bien adaptée au choix d'un seuil pour $R_{1,i}$. En effet, dans de nombreux cas, $R_{1,i}$ n'est pas une fonction concave du seuil de troncature appliqué aux coupes de référence. C'est par exemple le cas dans le modèle EPS des tranches 900MWe d'EDF où, lorsque EB_i correspond à la défaillance en fonctionnement d'une pompe spécifique, on se rend compte que pour un seuil compris entre $1,15 \cdot 10^{-12}$ et $9 \cdot 10^{-14}$, la valeur de $R_{1,i}$ n'évolue pas, comme on peut le voir dans la figure 1.17.

De plus, cette méthode nécessite la mise en œuvre d'une démarche itérative pour déterminer un seuil de troncature pour chaque valeur de i, c'est-à-dire pour chaque EB que l'on veut calculer. Elle est donc beaucoup trop coûteuse en ressources. Un autre processus de troncation du jeu de coupes est nécessaire.

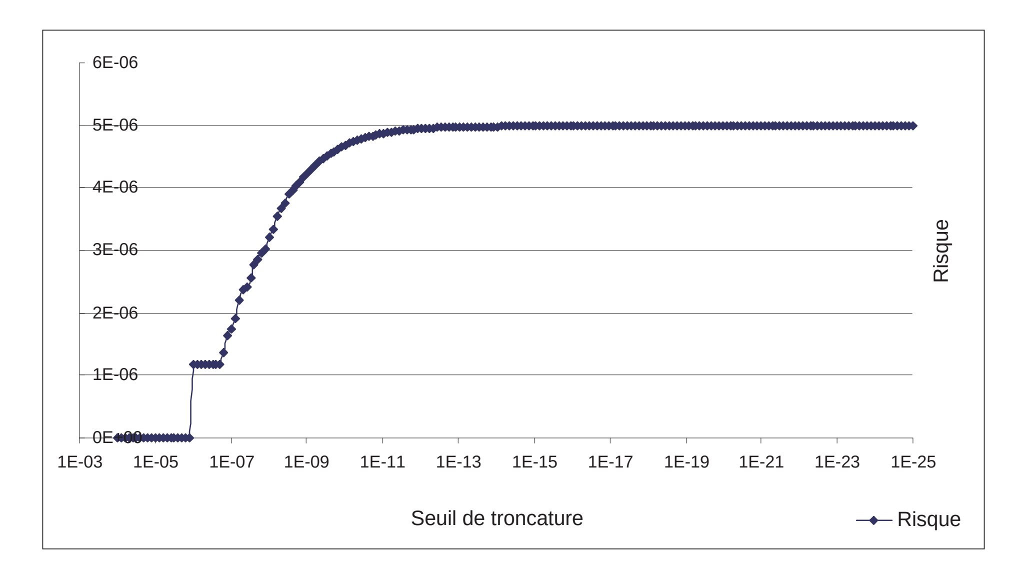


FIG. 1.16 – *Valeur du risque de référence en fonction du seuil de troncature probabiliste* S_p

Conclusion sur le calcul des facteurs d'importance à partir du jeu de coupes de référence : Le calcul des mesures d'importance en modifiant le jeu de coupes de référence est rapide et automatique. C'est donc une solution qui doit être développée. Toutefois, la taille de ce jeu de coupes conditionne la précision des facteurs d'importance qui en sont déduits. L'impact important de la troncation du jeu de coupes de référence sur le calcul des mesures d'importance est même identifié comme une limite majeure à leur application par Fleming dans le NUREG 6813 [49]. Ainsi, il souligne que "*Les logiciels supports des EPS sont programmés pour calculer les Risk Achievement Worth (RAW) à partir d'un jeu de coupes de référence tronqué et, dans ce cas, les RAW de certains événements peuvent être sous-estimés*". Il faut donc définir un processus de sélection des coupes de référence (un processus de troncation du jeu de coupes) qui garantisse l'absence de sous-estimations significatives des facteurs d'importance sans nécessiter un jeu de coupes trop important.

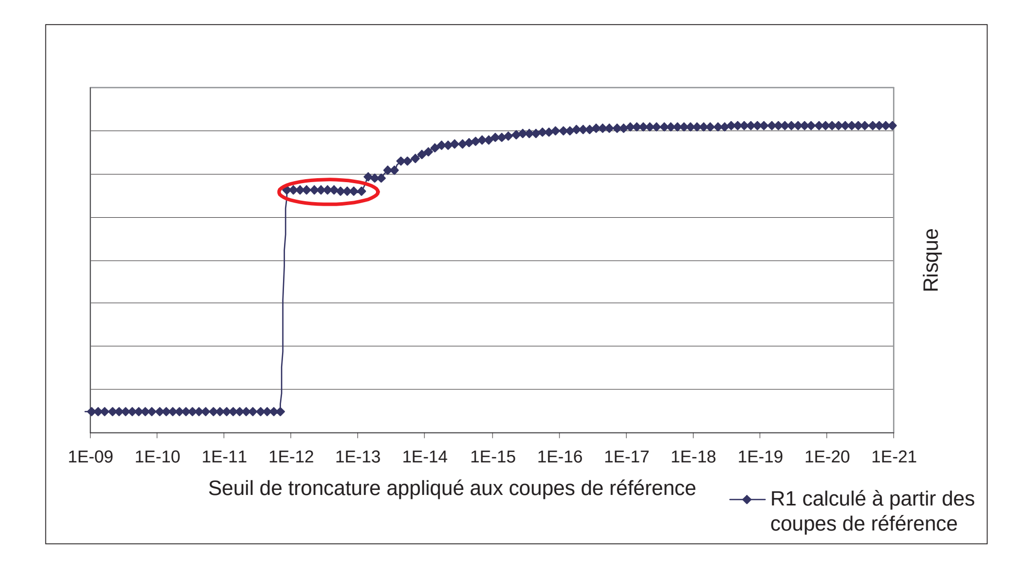


FIG. 1.17 – *Valeur de $R_{1,i}$ en fonction du seuil de troncature employé pour générer les coupes de référence à partir desquelles $R_{1,i}$ est calculé*

Approche alternative : modélisation au moyen de BDD et facteurs d'importance

Les outils supports d'une modélisation de type BDD ne recourent pas à la troncation de la fonction de structure [44, 45, 46]. Une modélisation de l'EPS au moyen d'un BDD supprimerait les incertitudes liées à la troncation du jeu de coupes. Comme on l'a vu dans la section 1.4.1 du chapitre 1, une EPS simplifiée pourrait être modélisée au moyen d'un BDD. Cette simplification n'aurait qu'un impact mineur sur l'estimation du risque de référence.

Toutefois, comme le souligne Epstein dans [46], cette simplification peut conduire à négliger les interdépendances entre systèmes et particulièrement les interdépendances dues aux systèmes supports, alors même que ces systèmes supports[13] interviennent dans de multiples points de nombreux arbres de défaillances des EPS.

Les événements correspondant à des défaillances au sein de ces systèmes supports peuvent être très importants pour le risque ou la sûreté. S'ils ne sont pas ou que partiellement modélisés, leur facteurs d'importance seront, à tort, très fortement sous-estimés voire nuls. Avec la modélisation actuelle des systèmes supports, les simplifications nécessaires à l'encodage d'une EPS sous forme de BDD pourrait donc conduire à sous-estimer très fortement l'importance de certains événements qui ne seront que partiellement ou pas du tout modélisés.

La mise en œuvre des applications des facteurs d'importance décrites dans la section 3.1 reste sujette à caution quand elle repose sur des facteurs d'importance calculés au moyen d'EPS simplifiées.

Pour plus d'informations, l'EPRI précise dans [40] quel doit être le niveau de détail nécessaire dans les EPS pour permettre leur utilisation dans des processus de décision incluant des facteurs d'importance.

4.2.2 Incertitudes liées aux simplifications pénalisantes des modèles

Comme on l'a vu en introduction, les modèles EPS d'EDF ont été initialement développés pour déterminer le risque de référence et les séquences prépondérantes. Des simplifications en adéquation avec ces deux objectifs ont été apportées. Acceptables dans le cadre du calcul du risque de référence, celles-ci peuvent devenir pénalisantes lorsque l'on veut calculer des facteurs

[13]Les systèmes supports sont des systèmes dont la fonction est de permettre le fonctionnement d'autres systèmes, par exemple les systèmes de distribution électrique ou pneumatique.

d'importance.

Exemple des initiateurs "valeur point" : Certains initiateurs correspondent à la défaillance d'un système. Leur probabilité d'occurrence dépend donc de la probabilité d'occurrence de plusieurs EB et de la fonction de structure ϕ modélisant l'état de ce système. Pourtant, dans les modèles EPS de référence, la probabilité d'occurrence de ces initiateurs est modélisée au moyen d'un seul EB (au lieu d'un arbre de défaillances). On parle alors d'initiateur "valeur point". La probabilité de défaillance de ces systèmes est calculée en dehors des modèles EPS, puis elle est attribuée à la "valeur point". Si la probabilité d'occurrence d'un EB intervenant dans l'arbre de défaillances d'un initiateur, par exemple EB_i, est modifiée, il faut remettre à jour à la main la valeur point. Lorsqu'on veut calculer $R_{1,i}$, on doit donc recalculer à la main la probabilité d'occurrence du ou des initiateurs qui dépendent entre autres de EB_i. On ne peut donc pas calculer automatiquement les mesures d'importance de tous les EB intervenant dans des initiateurs. Ainsi Fleming, dans le NUREG 6813 [49], précise que "*la démarche permettant d'utiliser des arbres de défaillances pour modéliser les initiateurs n'est que très peu appliquée par les exploitants dans leurs modèles EPS*".

C'est par exemple le cas de l'initiateur "perte du système d'Alimentation de Secours des Générateurs de vapeur (ASG)". Cet initiateur correspond à la perte d'un système et peut être modélisé au moyen d'un arbre de défaillances. Toutefois, dans certains modèles EPS, cet initiateur était modélisé au moyen d'une simple valeur point : $EB_{init\ ASG}$.

Cette modélisation, acceptable dans le cadre du calcul du risque de référence, pose problème lorsque l'on veut définir l'importance d'événements qui interviennent, par exemple, dans l'arbre de défaillances modélisant la perte de l'ASG. Lors du calcul automatique des facteurs d'importance de ces EB, RSW ne prendra pas en compte le fait que la probabilité de $EB_{init\ ASG}$ ne correspond plus à la probabilité d'occurrence de l'initiateur.

Exemple des sous-systèmes symétriques modélisés de manière dissymétrique : Les centrales nucléaires comportent de nombreux sous-systèmes appelés "voies", "files" ou "boucles" qui sont fonctionnellement et structurellement identiques. Ces sous-systèmes sont parfaitement symétriques et utilisés de manière symétrique. L'apparition de certains initiateurs (brèche primaire par exemple) peut survenir sur n'importe quelle boucle mais sera localisée, par choix de modélisation, sur une boucle particulière. De même, "*le fonctionnement de systèmes en redondance passive peut être toujours considéré dans le modèle en fonctionnement initial sur la voie ou file A lorsqu'il n'y a pas de voie ou de file préférentielle. Toute la probabilité est alors reportée sur la voie, boucle ou file ainsi particularisée*" [79]. Le calcul global du risque sera correct mais cette dissymétrie de modélisation faussera l'estimation de l'importance des matériels situés sur ces voies.

Le fait de considérer que la voie A est toujours en fonctionnement et que la voie B est toujours en secours, alors que dans les faits, la voie en fonctionnement est permutée tous les 15 jours, a pour conséquence d'augmenter artificiellement l'importance des EB modélisant la défaillance en fonctionnement de composants de la voie A. De même, l'importance des défaillances à la sollicitation des composants de la voie B sera sur-estimée.

Il en résulte que deux EB qui modélisent le même mode de défaillance de deux composants parfaitement symétriques appartenant à deux sous-systèmes parfaitement identiques, utilisés de manière symétriques, auront des facteurs d'importance différents.

Ces simplifications pénalisantes pour le calcul du risque de référence doivent être identifiées et une modélisation alternative, qui ne pose pas de problème lors du calcul des facteurs d'importance, doit pouvoir être proposée.

4.2.3 Incertitudes paramétriques

Les taux de défaillance à partir desquels les probabilités d'occurrence sont définies sont issus du retour d'expérience d'EDF. Ces paramètres de fiabilité correspondent à des événements peu probables, rarement observés. Du fait de ce manque de données, le retour d'expérience relativement à un événement se fait en agglomérant des événements survenus à des périodes différentes qui correspondent à des contextes qui évoluent (âge des matériels, règles de conduite et de maintenance, etc.). Ces estimateurs sont donc entachés d'incertitudes épistémiques [71].

De plus, la valeur de certains paramètres peut être intrinsèquement aléatoire. On ne peut donc pas considérer le risque de référence seul, mais on doit aussi s'intéresser à sa variabilité, qui dépend de la variabilité des probabilités d'occurrence des événements de base.

De nombreux travaux proposent de caractériser cette variabilité du risque de référence et de la prendre en compte dans les processus de prise de décision [14, 77, 43, 59]. Si les décisions fondées sur la valeur du risque de référence doivent inclure la variabilité de cette valeur, il doit en être de même pour les processus de décision basés sur les facteurs d'importance. Il faut donc pouvoir caractériser leur variabilité.

4.2.4 Simplifications imposées par RSW

Limites de l'hypothèse des événements rares

RSW ne propose qu'une approximation de Poincaré à l'ordre un, deux ou trois. On ne dispose pas, pour un jeu de coupes donné, de la probabilité exacte d'occurrence de l'une de ces coupes mais uniquement d'un majorant et d'un minorant (c.f. section 1.2.4 du chapitre 1).

L'absence d'un développement complet de Poincaré génère donc de l'incertitude sur les valeurs des facteurs d'importance.

Limitation imposée du nombre de coupes

Comme on l'a vu dans la section 1.2.5 du chapitre 1, l'utilisateur peut (en théorie) choisir les valeurs des seuils de troncature comme il l'entend. Ainsi, le nombre maximum de coupes généré, $S_{p,N}$, est censé pouvoir prendre n'importe quelle valeur de $\mathbb{N}$. Dans les faits, avec RSW 2.11 ou avec ses versions antérieures, on ne peut choisir une valeur de $S_{p,N}$ supérieure à 10 millions. Quoi qu'il advienne, avec RSW, on supprimera systématiquement les coupes dont la probabilité est inférieure à celle de la dix millionième coupe (avec les coupes classées par probabilité d'occurrence décroissante).

Ainsi, si la dix millionième coupe a une probabilité d'occurrence de 10^{-17}, même si un seuil absolu $S_{p,A}$ de 10^{-25} est fixé, toutes les coupes dont la probabilité est inférieure à 10^{-17} seront supprimées.

Non-reminimalisation du jeu de coupes lors du calcul de $\mathbf{R_{1,i}}$

Lorsque RSW effectue automatiquement le calcul des facteurs d'importance de EB_i, $R_{1,i}$ est calculé à partir du jeu de coupes de référence en le modifiant. Comme on l'a vu dans la section 4.2.1 du chapitre 1, le calcul de $R_{1,i}$ nécessite de modifier toutes les coupes contenant EB_i et de vérifier, pour toutes celles qui ne le contiennent pas, qu'elles restent minimales. Cette deuxième étape n'est pas faite par RSW, qui se contente d'estimer $R_{1,i}$ comme :

$$R_{1,i} \approx \frac{1}{P\left(EB_i\right)} \cdot \sum_{EB_i \in CM_j} P\left(CM_j\right) + \sum_{EB_i \notin CM_k} P\left(CM_k\right)$$

Dans la somme $\sum_{EB_i \notin CM_k} P\left(CM_k\right)$, toutes les coupes ne contenant pas EB_i sont prises en compte, y compris celles qui deviennent non minimales lorsque EB_i est certain.

Pour un jeu de coupes donné[14], la valeur de $R_{1,i}$ est doublement sur-estimée, premièrement parce que des coupes non minimales sont conservées, deuxièmement parce que $R_{1,i}$ est approché par un développement de Poincaré à l'ordre 1 qui est un majorant de $R_{1,i}$.

Un même événement modélisé avec deux EB

RSW associe à un EB une probabilité d'occurrence. Un même EB ne peut donc pas avoir une probabilité d'occurrence différente suivant le contexte.

Or, dans certains modèles, on peut considérer l'occurrence d'un mode de défaillance pour un matériel donné, pour des temps de mission différents. C'est en particulier le cas lorsqu'un événement contribue à la fois à l'occurrence d'un initiateur (calculée sur la durée sur laquelle l'initiateur peut se produire) et à l'occurrence de la défaillance d'un système support (calculée sur 24 heures). On est alors obligé, dans RSW, de modéliser ce même événement avec plusieurs EB : un par temps de mission. Ainsi, si l'occurrence d'un événement i est considérée sur un temps T_1, un temps T_2 et un temps T_3, on créera les EB : EB_{i,T_1}, EB_{i,T_2} et EB_{i,T_3}.

De plus, RSW les considérera comme indépendants. On peut ainsi trouver, dans un jeu de coupes issu de RSW, des coupes contenant $EB_{i,T_1} \cap EB_{i,T_2}$, alors que l'un implique l'autre. En effet, si on considère que l'initiateur s'est produit entre autres parce que l'événement i est réalisé, on doit considérer, dans les missions de sauvegarde, que cet événement est certain.

RSW calculera automatiquement des facteurs d'importance séparés pour ces trois EB, alors qu'il s'agit d'un même événement.

Prise en compte des défaillances de causes communes

Lorsque RSW calcule automatiquement les facteurs d'importance de chaque EB, il ne fait pas de différence entre les EB_{DCC} et les autres. On connaît ainsi l'importance de la défaillance en fonctionnement de la pompe 1 et de la pompe 3 par cause commune, ou l'importance de la défaillance intrinsèque de la pompe 1, mais on ne peut pas connaître l'importance de la défaillance de la pompe 1 tous modes de défaillance confondus. RSW ne calcule pas l'importance des modes communs ou d'un événement quelle qu'en soit la cause à partir de l'importance de chaque événement de base, comme on l'a vu dans la section 2.2 du chapitre 1.

Conclusion sur les simplifications imposées par RSW

Les simplifications présentées dans cette section compliquent l'interprétation des facteurs d'importance et/ou génèrent des imprécisions lors de leur calcul. Il faut donc pouvoir estimer leur impact et, le cas échéant, les corriger.

5 Axes de travail : réduire les incertitudes, considérer de nouveaux types d'événements et aider à la conception

Compte tenu de l'état de l'art et des diverses limites et besoins identifiés dans ce chapitre (cf. sections 3.2, 4.2.3, 4.2), trois axes potentiels de recherche apparaissent : la caractérisation et la recherche d'une gestion moins manuelle des incertitudes, l'étude de l'importance de macro-événements et non plus d'événements de base, et enfin l'emploi d'une méthode de type EPS de manière conjointe à l'approche déterministe lors de la conception de nouvelles centrales.

Incertitudes

Les facteurs d'importance interviennent dans des processus de prise de décision qui peuvent avoir un réel impact sur le risque. Il faut donc être sûr de prendre la "bonne décision". On ne peut ainsi pas accepter que les facteurs d'importance soient entachés d'incertitudes qui faussent

[14] Ce "jeu de coupes donné" peut ne pas être complet. Il ne faut pas oublier qu'il est souvent tronqué et que la probabilité qui en est issue est donc sous-estimée.

la perception du risque. Ces incertitudes sont stochastiques (incertitudes sur les paramètres) ou épistémiques [71] (incertitudes liées aux simplifications de RSW, incertitudes liées aux simplifications de modèle).

La caractérisation du comportement stochastique des paramètres d'entrée des EPS n'est pas aisée car on ne dispose que de petits échantillons (peu d'événements observés) issus du retour d'expérience. De plus, EDF travaille déjà par ailleurs, en partenariat avec l'EPRI (Electric Power Research Institute), sur le sujet. Nous avons donc décidé de ne pas prendre en compte ces incertitudes dans nos travaux de thèse.

En revanche, les incertitudes épistémiques liées aux simplifications de RSW ou aux simplifications faites lors de la modélisation doivent être étudiées, en vue de permettre la résorption ou, a minima, la caractérisation de celles qui ont un impact non négligeable sur l'incertitude des facteurs d'importance. C'est un préalable à l'utilisation des facteurs d'importance dans des processus de prise de décision.

Les facteurs d'importance étant utilisés dans un contexte industriel, ils doivent être calculés de manière simple, rapide et automatique tout en identifiant ceux qui sont le plus entachés d'incertitudes.

Toutes les sources d'incertitudes identifiées ne doivent pas être traitées de la même manière. Si les incertitudes liées à des simplifications de modélisation doivent être supprimées, celles qui sont liées à la troncation du jeu de coupes de référence doivent être le plus possible limitées, et les quelques facteurs d'importance fortement impactés doivent être très localisés et clairement identifiés. Enfin, dans la mesure où l'hypothèse des événements rares s'avère fondée (le développement de Poincaré à l'ordre 1 et à l'ordre 2 de R, $R_{1,i}$ ou $R_{0,i}$ donne des valeurs très proches), l'incertitude liée à cette hypothèse sera acceptée.

Facteurs d'importance pour des événements composites

Pour pouvoir développer de nouvelles applications utilisant les facteurs d'importance, on ne peut pas se satisfaire uniquement de la connaissance de chaque EB considéré individuellement. Comme on l'a vu dans ce chapitre, dans la section 2.3, il existe des extensions des facteurs d'importance à des macro-événements pouvant être exprimés à partir de plusieurs événements de base. Toutefois, leur définition reste partielle et leurs applications potentielles sont encore à définir.

Approche probabiliste et conception

Même si l'application d'une démarche déterministe lors de la conception des centrales actuellement en exploitation a donné de bons résultats en termes de sûreté, l'utilisation, non plus seule, mais conjointe de ce type de démarches avec une approche de type EPS sera mise en œuvre pour la conception des futures centrales. Cette utilisation conjointe des deux démarches reste très largement à concevoir, et semble offrir une opportunité à la définition et à l'utilisation de facteurs d'importance.

Chapitre 2

Réduire les incertitudes et "industrialiser" le calcul des mesures d'importance

Les mesures d'importance sont utilisées dans des applications ayant un impact sur la sûreté, elles doivent être calculées de manière précise. Chaque modification du modèle EPS modifie la valeurs de toutes les mesures d'importance de tous les EB. Elles sont donc toutes re-calculées après chaque mise à jour du modèle. Il faut donc pouvoir garantir la précision de ces mesures d'importance tout en automatisant et accélérant leur calcul le plus possible. Enfin, un mode de calcul simple et ergonomique doit permettre une meilleure utilisation de ces indicateurs.

1 Réduire les incertitudes dues à la modélisation

Des simplifications de modélisation (modélisation dissymétrique, utilisation de "valeurs point") ont été faites lors du développement des modèles de référence car elles ne nuisent pas ou peu à la précision du calcul du risque de référence. Elles contribuent ainsi à maîtriser la taille des modèles EPS sans impacter la valeur du risque de référence, mais elles sont en revanche pénalisantes lorsque l'on veut calculer des facteurs d'importance. Il convient donc de les corriger.

De nombreuses simplifications de modèle impactant le calcul des facteurs d'importance existent. On peut retrouver l'ensemble des simplifications identifiées et traitées durant cette thèse dans la note [30]. Elle présente l'approche d'EDF pour contrôler les incertitudes sur les facteurs d'importance et fait partie des contributions d'EDF à l'EPRI (Electric Power Research Institue).

L'ensemble de ces travaux sera présenté, dans ce mémoire, au moyen de deux exemples illustratifs :
- le cas des initiateurs correspondant à des défaillances de systèmes et modélisés au moyen de valeurs point,
- le cas des sous-systèmes symétriques modélisés de manière dissymétrique.

1.1 Modélisation des événements initiateurs au moyen d'arbres de défaillances

Rappel du problème

Certains initiateurs correspondent à des défaillances de systèmes et peuvent être modélisés au moyen d'un arbre de défaillances. Pourtant, ils sont représentés au moyen d'un seul EB appelé "valeur point" et ayant pour probabilité la probabilité d'occurrence de la porte sommet de cet arbre de défaillances.

Lorsqu'on veut calculer l'importance d'un EB qui aurait dû intervenir dans cet arbre de défaillances, on la sous-estime beaucoup. En effet, un EB présent dans un initiateur se retrouvera dans toutes les séquences de l'arbre d'événements associé à cet initiateur. C'est à dire que toutes les trajectoires accidentelles débutant par cet initiateur contiendront cet EB. L'occurrence ou la non-occurrence certaine de cet EB impactera donc toutes les séquences de l'arbre d'événements. Dans le NUREG 6813 [49], on peut ainsi lire que les modèles EPS "*échouent à estimer l'importance d'un équipement* [dont la défaillance] *cause l'occurrence d'un initiateur*".

Solution

L'arbre de défaillances correspondant à l'occurrence de l'initiateur doit se substituer à la valeur point.

Le développement de ces arbres de défaillances modélisant l'occurrence d'initiateur implique qu'on ne considère plus systématiquement la probabilité d'occurrence de toutes les défaillances sur 24 heures. En effet, le principe d'une EPS est de quantifier, pour chaque arbre d'événements, la probabilité d'occurrence d'un initiateur sur un cycle du combustible et la probabilité (sachant que cet initiateur s'est produit) de défaillance des missions de sauvegarde qui y sont associées durant 24 heures. Dans un arbre de défaillances modélisant un initiateur, la probabilité de défaillance en fonctionnement des matériels concernés est donc calculée sur une durée correspondant au temps de fonctionnement de ces matériels sur un cycle. Si certains EB sont dans des arbres de défaillances modélisant l'échec de missions de sauvegarde et dans un arbre de défaillances modélisant l'occurrence d'un initiateur, leur probabilité de défaillance sera tantôt calculée sur 24 heures et tantôt sur un cycle du combustible.

Par exemple, la pompe ASG 1 intervient dans plusieurs missions de sauvegarde. On crée donc un EB nommé EB_{ASG1PO_DF} qui modélise la défaillance en fonctionnement de la pompe ASG 1. Dans un arbre de défaillances d'une mission de sauvegarde, on calcule la probabilité d'occurrence de cet EB au bout de 24 heures. Cette même pompe intervient dans l'initiateur "perte ASG état A4". Dans le modèle EPS des centrales de 900MWe d'EDF, l'état A4 correspond à l'arrêt à chaud et dure en moyenne 87 heures sur une année. Dans cet état, la pompe ASG 1 est toujours en fonctionnement. La probabilité d'occurrence de l'événement "défaillance de la pompe ASG en fonctionnement" doit donc être calculée en considérant une durée T_{A4} de 87 heures[1]. On crée donc un autre EB nommé $EB_{ASG1PO_DF,T_{A4}}$ dont la probabilité d'occurrence est calculé sur 87 heures. Ce second EB est utilisé dans l'arbre de défaillances modélisant l'occurrence de l'initiateur.

Problème induit par une meilleure modélisation des initiateurs

La défaillance d'un même événement EB_i ne peut, dans la plupart des logiciels supports des EPS, être considérée sur des temps de mission différents (cf. page 4.2.4). On est obligé de créer plusieurs EB (EB_{i,T_1}, EB_{i,T_2} et EB_{i,T_3}) pour considérer la probabilité d'EB_i aux temps T_1, T_2 et T_3. De plus, RSW considérera à tort que les événements EB_{i,T_1}, EB_{i,T_2} et EB_{i,T_3} sont indépendants. Fleming souligne ce problème dans [49] en précisant que "*le problème* [est

[1] $P\,(def.\ pompe\ ASG) = 1 - \exp\left(-\lambda_{ASGPO} \cdot T_{A4}\right)$ avec λ_{ASGPO} le taux de défaillance de la pompe ASG 1

dû à] *l'inaptitude à considérer les interdépendances entre les arbres de défaillances d'un même système présent dans un initiateur et dans une fonction de mitigation*”.

Si on reprend l'exemple du paragraphe précédent, on doit créer l'événement de base $EB_{ASG1PO_DF,T_{A4}}$ qui correspond à la probabilité de défaillance de la pompe ASG 1 dans l'état A4 et l'événement de base EB_{ASG1PO_DF} qui correspond à la défaillance de la pompe ASG 1 calculée sur 24 heures. On peut alors avoir des coupes contenant ces deux EB, ce qui n'a aucun sens physique. En effet, on ne peut pas, sachant que la défaillance de la pompe a provoqué l'occurrence de l'initiateur, considérer que le fonctionnement de cette pompe peut contribuer au bon fonctionnement d'une parade de ce même initiateur. Le second événement (EB_{ASG1PO_DF}) est inclus dans le premier ($EB_{ASG1PO_DF,T_{A4}}$).

Solution complémentaire

Pour prévenir l'existence de coupes contenant la défaillance d'un même matériel considérée à différents instants, nous avons mis en place des règles de correction des coupes. Ainsi, dans toute coupe contenant plusieurs fois le même EB considéré sur plusieurs instants différents, seul le plus probable de ces EB y est conservé. Les autres sont supprimés de la coupe et la probabilité de celle-ci est ré-évaluée.

1.2 Modélisation dissymétrique de systèmes symétriques

Rappel du problème

“*Certains systèmes symétriques utilisés de manière symétrique sont modélisés de manière dissymétrique*” [79].

Par exemple, deux voies (A et B) identiques en redondance passive l'une par rapport à l'autre peuvent être régulièrement permutées (tantôt la voie A est en fonctionnement et la B en secours, et tantôt c'est l'inverse). Pourtant, pour éviter d'avoir à considérer le cas ou B est en fonctionnement et A en secours, la voie A sera toujours considérée en fonctionnement et la voie B sera toujours en secours. Cette simplification divise par deux la taille de l'arbre de défaillances modélisant la perte des deux voies. Cette simplification aura pour impact de sur-estimer la contribution au risque des événements correspondant à la défaillance en fonctionnement de la voie A et les événements modélisant la défaillance à la sollicitation, quand la voie A défaille, de la voie B.

Solution

Toutes les modélisations artificiellement dissymétriques sont identifiées. Celles qui peuvent être rendues symétriques doivent l'être [30]. Lorsque cette symétrisation représente une trop grande quantité de travail au vu du gain en termes de précision, tous les EB symétriques doivent être identifiés. Pour chaque ensemble d'EB symétriques, l'importance de chacun d'eux est majorée par l'importance de l'EB le plus important de l'ensemble. Il s'agit d'une approche conservative mais simple de mise en œuvre.

Exemple : Dans l'exemple de la figure 2.1, on suppose que les pompes 1 et 2 sont identiques, de même pour les vannes 1 et 2. On suppose de plus que ces deux voies sont en redondance passive et que la voie en marche est permutée tous les 15 jours.

Pour ne pas avoir à modéliser le cas où la voie A est en fonctionnement et le cas où c'est la voie B, l'analyste EPS a considéré que la voie A était toujours en fonctionnement et la voie B toujours en secours. Il a donc produit l'arbre de défaillances de la figure 2.2.

Dans cet arbre de défaillances, la défaillance à la sollicitation de la pompe 1 (suite à la perte de la voie B) n'est même pas considérée et la défaillance en fonctionnement de la pompe 2 n'est considérée que sur le temps de repli de l'installation (dans cette modélisation, on ne se sert de

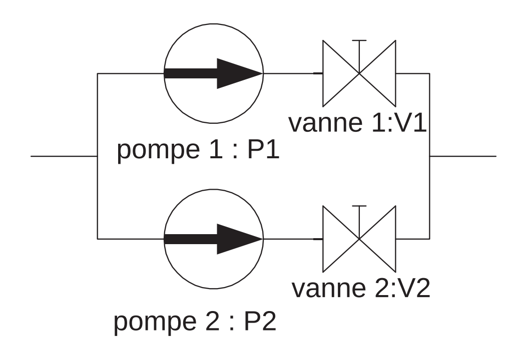


Fig. 2.1 – *Exemple d'une portion de système contenant deux voies symétriques*

Fig. 2.2 – *Modélisation simplifiée (dissymétrique) du sous-système de la figure 2.1*

la pompe 2 que pour revenir à l'état sûr. On ne s'en sert pas pour produire).

Pour calculer, par exemple, le FDR de la pompe 1 et de la pompe 2, les FDR des EB EB_{P1_DF} et EB_{P2_DF} sont calculés automatiquement, puis on considère que les FDR de la pompe 1 et de la pompe 2 sont majorés par la plus grande de ces deux valeurs. C'est à dire que de manière conservative, on considère que :

$$FDR_{majoré}\left(EB_{P1_DF}\right) = \max\left(FDR_{calc.}\left(EB_{P1_DF}\right), FDR_{calc.}\left(EB_{P2_DF}\right)\right)$$

Sous certaines conditions, nous avons pu montrer que la "vraie" valeur de l'importance d'EB symétriques (sans dissymétrie simplificatrice) correspond à la moyenne arithmétique des importances calculées [30]. Ce résultat n'étant pas robuste, nous ne l'avons pas diffusé.

2 Générer et traiter les bonnes données pour calculer les mesures d'importance

Les simplifications algorithmiques faites dans les logiciels supports (troncation du jeu de coupes de référence, non reminimalistion du jeu de coupes lors du calcul des $R_{1,i}$ etc.) des EPS génèrent des biais systématiques sur les valeurs des facteurs d'importance [49, 19, 48, 32, 44, 46, ...].

La correction de ces biais dûs aux algorithmes de RSW a toujours été faite à la main pour chaque événement de base. Cette démarche est longue, donc coûteuse, et peut laisser place à des erreurs de manipulation du modèle EPS. Une démarche plus automatique, plus simple et plus ergonomique doit être développée.

La section 2.1 présente notre démarche générique d'obtention d'un jeu de coupes de référence qui permet un calcul rapide et précis des facteurs d'importance. La section 2.2 présente l'outil que nous avons développé pour calculer tous les facteurs d'importance à partir de ce jeu de coupes, et fournir automatiquement toutes les informations nécessaires à leur utilisation.

2.1 Un processus de troncation adapté au calcul rapide et précis des mesures d'importance

Les mesures d'importance ne peuvent pas être calculées en générant, à partir du modèle, un jeu de coupes correspondant à $R_{1,i}$ et un autre correspondant à $R_{0,i}$ pour chaque EB car cette approche est beaucoup trop longue et trop coûteuse en main d'œuvre (cf. section 4.2.1 du chapitre 1).

Un calcul automatique et plus rapide de ces valeurs doit être effectué à partir d'un même jeu de coupes : le jeu de coupes de référence[2]. Les processus de troncation probabiliste existant dans RSW permettent de conserver les coupes significatives pour le risque de référence R. Ces coupes ne sont pas forcément celles qui sont significatives pour le calcul de $R_{1,i}$ [19, 48, 84]. En effet, on a vu que moins l'EB étudié est probable, plus le jeu de coupes nécessaire pour un calcul sans biais significatif de $R_{1,i}$ est dissemblable de celui nécessaire pour un calcul de R sans biais.

L'objectif est d'avoir un jeu de coupes de référence permettant de calculer à la fois R, $R_{1,i}$ et $R_{0,i}$ sans biais significatif et quel que soit i. La solution la plus simple (car c'est celle mise en œvre dans la plupart des logiciels supports des EPS [49]) semble être d'utiliser un processus de troncation probabiliste simple[3] et de diminuer la valeur du seuil probabiliste S_p jusqu'à garder toutes les coupes significatives pour R et $R_{0,i}$ (ce sont les mêmes) ainsi que les coupes qui deviennent significatives lorsqu'on calcule $R_{1,i}$, c'est à dire les coupes qui deviennent significatives lorsque EB_i est certain quel que soit i. Comme nous allons le voir dans la section suivante, cette solution n'est pas optimale.

[2]les coupes correspondant au risque de référence

[3]Un processus où les coupes sont conservées ou supprimées en comparant leur probabilité de référence à un seuil fixé.

2.1.1 *Comment baisser le niveau de troncation et pourquoi ce n'est pas une solution optimale*

Comment choisir la valeur du seuil

Pour choisir la valeur du seuil probabiliste S_p utilisé pour générer un jeu de coupes de référence utilisé ensuite pour le calcul des mesures d'importance de tous les EB , il faut connaître, pour une valeur de S_p, quelle est la sous-estimation de $R_{1,i}$, de $R_{0,i}$ et de R pour tout i. On peut alors diminuer la valeur de S_p jusqu'à ce que la sous-estimation de ces trois valeurs soit acceptable.

On peut diminuer la valeur du seuil de troncature pour déduire la valeur d'un majorant de la sous-estimation de $R_{1,i}$ ($\Delta_{TRM;1,i}$) de celle de R (Δ_{TRM}). Mais, cette valeur étant un bien trop grand majorant de l'erreur réellement commise sur le risque de référence Δ_{TR}, on ne peut pas avoir un majorant de $\Delta_{TR;1,i}$ qui soit réaliste. Il faut donc trouver une autre façon d'apprécier la sous-estimation de $R_{1,i}$, de $R_{0,i}$ et de R pour pouvoir fixer le seuil.

Une autre solution serait de reprendre la méthode proposée par Čepin dans [19]. Toutefois, comme on l'a déjà remarqué (cf. page53), la concavité de $R_{1,i}$ en fonction du seuil n'est pas vérifiée en pratique et cette méthode peut nécessiter une quantification trop fréquente du modèle EPS.

C'est pourquoi nous proposons une nouvelle approche de sélection du seuil, améliorant l'approche proposée par Čepin [19] en l'appliquant globalement à un groupe d'EB.

Choisir la valeur du seuil à partir de la somme des $R_{1,i}$: Si l'incertitude sur R due à la troncation est acceptable, alors celle sur $R_{0,i}$ l'est aussi. On doit donc trouver un seuil S_p pour lequel l'incertitude sur R et sur $R_{1,i}$ $\forall i$ reste acceptable.

La valeur du seuil de troncature qui permet de calculer R sans trop le sous-estimer est déjà connue, c'est le seuil utilisé communément pour générer les coupes de références (en général, il est compris entre 10^{-12} et 10^{-14} [48, 52]). Quelle que soit la valeur du seuil choisie, elle doit être inférieure ou égale à cette valeur pour que R et $R_{0,i}$ soient bien estimés (quel que soit i).

Il reste à déterminer la valeur de S_p pour laquelle les $R_{1,i}$ ne sont pas trop sous-estimés et ce, quel que soit i (puisqu'on veut utiliser ce jeu de coupes pour le calcul des mesures d'importance de tous les EB).

Pour ce faire, nous sommes partis du constat suivant : chaque $R_{1,i}$ calculé à partir des coupes de référence est une fonction monotone décroissante de la valeur du seuil de troncature appliqué à ce jeu de coupes.

De ce constat, on peut tirer les deux conclusions suivantes :

- la somme des $R_{1,i}$ calculés à partir des coupes de référence est une fonction monotone décroissante de la valeur du seuil de troncature appliqué à ce jeu de coupes (une fonction monotone croissante de $-\log(S_p)$),
- si, pour une valeur S_p donnée, la somme des $R_{1,i}$ exprimée en fonction de moins log du seuil a atteint son asymptote (en supposant qu'elle existe), alors tous les $R_{1,i}$ ont atteint la leur.

En faisant l'hypothèse que la somme des $R_{1,i}$ calculés à partir des coupes de référence est une fonction concave de la valeur du logarithme du seuil de troncature appliqué à ce jeu de coupes, et en se souvenant que cette fonction est de plus monotone croissante, on en déduit que si elle connaît un palier pour une valeur donnée, alors cette valeur correspond à son asymptote. Cette hypothèse est vérifiée empiriquement en dessous d'une certaine valeur de seuil, comme le montre l'annexe B page 166.

Sous cette hypothèse, on peut définir la **démarche de choix du seuil** d'un processus de troncature simple de la manière suivante :

1. La valeur du seuil de troncature S_p est diminuée pas à pas (S_{p_k} correspond à la valeur de

S_p à la $k^{\text{ème}}$ itération). Quand l'augmentation entre la valeur de $\sum_{i=1}^{n} R_{1,i}$ calculée avec le seuil S_{p_k} et celle calculée avec le seuil $S_{p_{k+1}}$ devient négligeable, S_{p_k} est considéré comme une valeur acceptable du seuil pour le calcul des $R_{1,i}$.

2. La même démarche est effectuée pour le risque de référence. Quand l'augmentation de la valeur de R calculée avec le seuil S_{p_j} et celle calculée avec le seuil $S_{p_{j+1}}$ devient négligeable, S_{p_j} est considéré comme acceptable pour le calcul du risque de référence.
3. la plus petite valeur entre S_{p_k} et S_{p_j} est sélectionnée comme seuil de troncature acceptable pour le calcul des facteurs d'importance.

Exemple : Dans le modèle EPS des centrales de 900 MWe, seuls deux EB ont une probabilité de défaillance inférieure à 10^{-10}. On suppose que la valeur de $R_{1,i}$ pour ces deux EB n'est pas considérée. On peut alors tracer la somme des $R_{1,i}$ en fonction du seuil pour les autres EB avec la somme des $R_{1,i}$ approximée par :

$$f\left(seuil\right) = \sum_{\substack{EB_i \\ Q(EB_i)\geq 10^{-10}}} \left(\sum_{Q(Coupe_l)\geq seuil} Q\left(Coupe_l/EB_i\right) \right)$$

On obtient alors la figure 2.3. A l'examen de cette figure, on se rend compte qu'un seuil de troncature de 10^{-20} permet d'atteindre la valeur qui parait être stationnaire de la courbe.

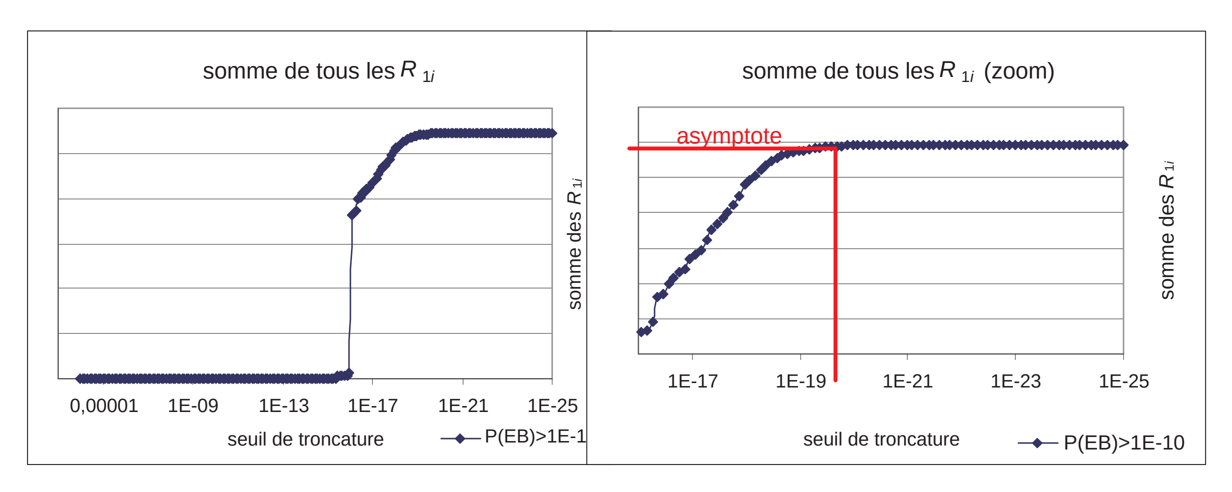


FIG. 2.3 – *Somme des $R_{1,i}$ des EB dont le probabilité d'occurrence est supérieure à 10^{-10} en fonction du seuil*

Validité de ce processus de choix de la valeur du seuil : Pour démontrer que ce processus est recevable, la seule obligation est de démontrer le caractère concave de $\sum_{i=1}^{n} R_{1,i}$ exprimé en fonction du seuil de troncature. Cette propriété n'est pas démontrable sur le plan théorique mais elle semble vérifiée avec les modèles EPS d'EDF, comme le montrent les figures présentées dans l'annexe B page 166.

Limite d'un processus de troncature simple

Lorsqu'on utilise un processus de troncation probabiliste simple il faut diminuer la valeur du seuil probabiliste S_p jusqu'à garder toutes les coupes significatives pour R et $R_{0,i}$ ainsi que

les coupes qui deviennent significatives lorsqu'on calcule $R_{1,i}$ quel que soit i. Certaines coupes qui deviennent significatives lorsque EB_i est certain peuvent avoir une faible probabilité de référence si cet EB a une faible probabilité de référence. Pour pouvoir tout de même les garder il faut que la valeur de S_p soit très petite. Cependant avec une troncation probabiliste simple et un seuil S_p élevé, on gardera aussi de nombreuses coupes négligeables pour le calcul de R et de $R_{0,i}$ qui restent négligeables lorsque l'un des EB qui compose ces coupes est certain. C'est le cas des coupes de référence qui ont une probabilité d'occurrence faible ($<10^{-15}$) et qui contiennent de nombreux EB dont la probabilité d'occurrence est relativement élevée ($\geq 10^{-4}$). Ces coupes, inutiles lors du calcul des mesures d'importance, sont longues à générer, consomment l'espace mémoire de l'ordinateur servant à les déterminer et ralentissent le calcul des mesures d'importance.

Exemple : Avec le modèle EPS de niveau 1 des centrales 900 MWe d'EDF, un seuil de troncature de 10^{-20} est nécessaire pour générer un jeu de coupes de référence à partir duquel la majorité des EB voient leurs facteurs d'importance peu sous-estimés du fait de la troncation du jeu de coupes (cf. figure 2.3). Comme on peut le voir sur la figure 2.4, 75 millions de coupes sont générées lorsqu'on utilise cette valeur de seuil.

Un tel jeu de coupes ne peut être généré en une seule fois (RSW ne peut générer qu'au plus dix millions de coupes par analyse) et le fractionnement de ce calcul est long, essentiellement manuel et donc source d'erreurs. De plus, la quantité de données générées est très importante et est donc difficile à traiter avec des moyens informatiques "standard". Enfin, à partir de ces très nombreuses coupes, le calcul de l'importance de chaque EB s'avère très long.

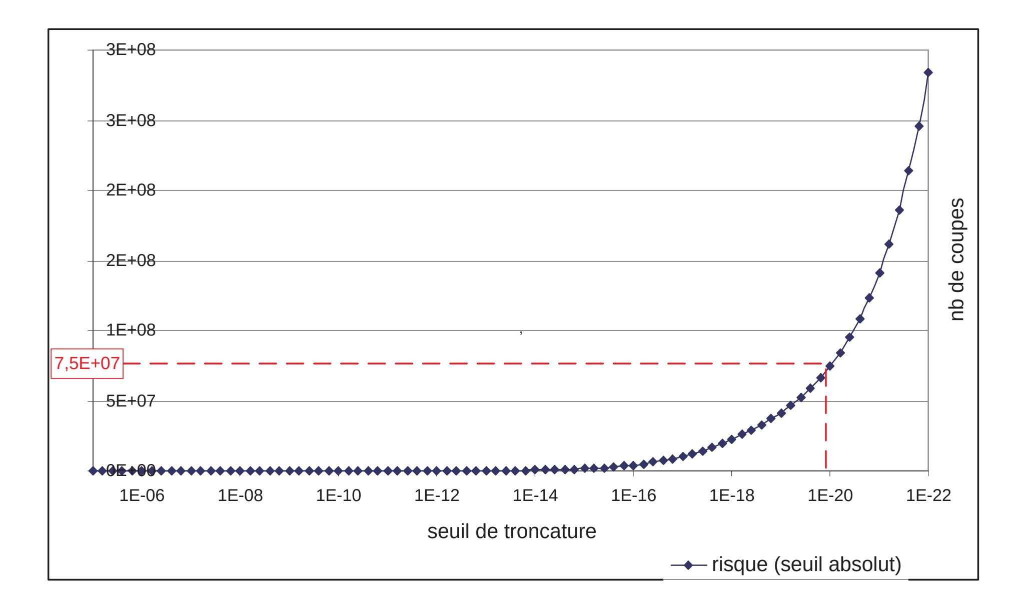


FIG. 2.4 – *Nombre de coupes de référence supérieures au seuil de troncature en fonction de sa valeur pour le modèle EPS des centrales de 900 MWe*

Il serait utile de définir un nouveau processus de troncation qui supprime les coupes qui ne sont significatives ni pour le risque de référence ni pour le calcul de l'importance des EB, tout en gardant toutes les autres.

2.1.2 Un processus de troncation double pour le calcul des mesures d'importance

Notre objectif est de calculer le risque de référence et l'importance de chaque EB à partir d'un seul jeu de coupes.

Pour que les calculs à partir de ce jeu de coupes soient rapides, il faut que celui-ci ne contienne que les coupes significatives pour le risque de référence, pour le calcul de $R_{1,i}$ et pour le calcul de $R_{0,i}$, et ce, quel que soit i. On pourra toutefois tolérer que certains EB, peu nombreux, ne soient pas calculés de manière précise s'ils sont identifiés. On pourra alors calculer leur importance “à la main” en générant, à l'aide du modèle, un jeu de coupes spécifique correspondant à $R_{1,i}$ et $R_{0,i}$ pour chacun d'eux.

Comme on l'a vu, les coupes significatives pour le risque de référence et pour le calcul de $R_{0,i}$ sont les mêmes. Pour les obtenir, il suffit d'appliquer le processus de troncation communément employé dans les modèles EPS de référence (en utilisant un processus de troncation probabiliste simple avec un seuil S_p égal à 10^{-12} par exemple).

Il reste donc à enrichir ce processus de troncation du jeu de coupes pour obtenir aussi les coupes significatives pour le calcul de $R_{1,i}$.

Un processus de troncation double basé et sur la probabilité de référence des coupes et sur leur probabilité potentielle

La décision de supprimer ou de conserver une coupe dans le jeu de coupes de référence utilisé pour le calcul de l'importance de chaque EB doit aussi reposer sur ce que nous appelons sa probabilité potentielle, et pas seulement sur sa probabilité de référence[4]. Nous définissons la probabilité potentielle d'une coupe comme :

Probabilité potentielle : *La probabilité potentielle d'une coupe correspond à la probabilité qu'aurait cette coupe si parmi les EB composant cette coupe, le moins probable devenait certain.*

Le probabilité potentielle d'une coupe j se calcule donc à partir de sa probabilité de référence comme :

$$\textit{probabilité potentielle}_j = \max_{\substack{EB_i \\ EB_i \in CM_j}} \left[P\left(CM_j/EB_i\right)\right] = \frac{P\left(CM_j\right)}{\min_{\substack{EB_i \\ EB_i \in CM_j}} \left[P\left(EB_i\right)\right]}$$

Nous introduisons la notion de seuil sur la probabilité potentielle. Ce seuil, que nous appelons S_{pot}, est un réel compris entre 0 et 1 dont la valeur est fixée par l'utilisateur. Nous reprenons de plus le principe d'un seuil probabiliste absolu (cf. 17).

À l'aide de ce nouvel outil, nous définissons alors le processus de troncation double suivant que nous avons initialement présenté dans la référence [32] :
Une coupe j est conservée dans le jeu de coupes si “*sa probabilité potentielle est supérieure à la valeur du seuil de troncation potentiel S_{pot} fixé par l'utilisateur*” [32]. C'est à dire si :

$$\exists i \text{ tel que } P\left(CM_j/EB_i\right) \geq S_{pot} \quad \Leftrightarrow \quad P\left(CM_j\right) \geq S_{pot} \cdot \min_{\substack{EB_i \\ EB_i \in CM_j}} \left[P\left(EB_i\right)\right]$$

ou si “*sa probabilité de référence est supérieure au seuil de troncation probabiliste absolu $S_{p,A}$ fixé par l'utilisateur*” [32], c'est-à-dire si :

$$P\left(CM_j\right) \geq S_{p,A}$$

En résumé, avec le processus de troncation que nous proposons, une coupe est conservée si :

$$P\left(CM_j\right) \geq \min\left(S_{p,A}; \left[S_{pot} \cdot \min_{\substack{EB_i \\ EB_i \in CM_j}} \left[P\left(EB_i\right)\right]\right]\right)$$

On obtient alors un processus de troncation double dans la mesure où il repose à la fois sur la probabilité des coupes de référence mais aussi sur leur probabilité potentielle.

[4]La probabilité qu'a cette coupe dans le cadre du calcul du risque de référence.

Majorant de l'incertitude de $R_{1,i}$ calculé avec cette méthode

Supposons que Δ_{TR,S_x} soit l'incertitude sur le risque de référence lorsque le jeu de coupes utilisé pour calculer ce risque est tronqué avec un seuil absolu S_x.

Pour une valeur de S_{pot} et de $S_{p,A}$ donnée, lorsque le processus de troncation que nous proposons est employé, on peut écrire :

$$\Delta_{TR_{1,i}} \leq \Delta_{TR,S_{p,A}} + \min\left(\frac{\Delta_{TR,S_{p,A}}}{p_i} ; \frac{\Delta_{TR,(S_{pot} \cdot p_i)}}{p_i}\right)$$

avec p_i la probabilité d'occurrence de EB_i.

En effet, parmi les coupes supprimées lors de la troncation, certaines contiennent EB_i d'autres pas.

Supposons que toutes les coupes supprimées par notre processus de troncation double contiennent EB_i. Dans ce cas, la probabilité potentielle d'une coupe j est supérieure ou égale à $P(CM_j/EB_i)$. Une coupe est donc supprimée si sa probabilité de référence est inférieure à $S_{p,A}$ et à $S_{pot} \cdot p_i$. Sous cette hypothèse, le majorant de la sous-estimation serait donc :

$$\min\left(\frac{\Delta_{TR,S_{p,A}}}{p_i} ; \frac{\Delta_{TR,(S_{pot} \cdot p_i)}}{p_i}\right)$$

Supposons maintenant qu'aucune coupe supprimée lors de la troncation double ne contiennent EB_i. Dans ce cas on ne peut pas majorer leur probabilité potentielle mais on sait que leur probabilité est inférieure à $S_{p,A}$. Sous cette hypothèse, le majorant de la sous-estimation serait donc : $\Delta_{TR,S_{p,A}}$.

Comme, en général, aucune de ces hypothèse n'est validée, on doit donc se placer dans le pire cas en sommant ces deux majorants.

Comparaison avec l'approche "manuelle"

Le but de ce paragraphe est de comparer l'incertitude sur $R_{1,i}$ lorsque cette valeur est calculée à la "main", en modifiant le modèle de référence pour créer un modèle dédié (un modèle où l'événement EB_i est certain) à l'incertitude lorsque $R_{1,i}$ est calculé à partir d'un jeu de coupes tronqué à l'aide du seuil S_{pot} basée sur la probabilité potentielle des coupes. On compare donc notre approche à une approche plus manuelle, mais jusqu'ici plus précise. (Pour plus d'informations sur cette approche "manuelle", on peut se reporter à la page 49).

Supposons que la valeur de S_{pot} soit égale à la valeur du seuil de troncature probabiliste S_p utilisé dans le modèle dédié et que $S_{p,A}$ vale 1 (seul la probabilité potentielle des coupes est prise en compte lors de la troncation double). Dans ce cas, on peut voir que $\Delta_{TR_{1,i}}$ est plus petit lorsque $R_{1,i}$ est calculé à partir d'un jeu de coupes de référence issu de notre méthode de troncation que lorsqu'il est calculé à partir d'un modèle dédié.

En effet, avec l'approche "manuelle", une coupe de référence CM_j contenant EB_i est gardée si $P(CM_j/EB_i) \geq S_p$. Avec notre approche, cette même coupe j est gardée si sa probabilité potentielle est supérieure à S_{pot} (avec $S_{pot} = S_p$). Puisque la coupe j contient l'EB_i on sait que l'EB le moins probable de la coupe a une probabilité d'occurrence au moins inférieure ou égale à $P(EB_i)$. Sa probabilité potentielle est donc supérieure ou égale $P(CM_j/EB_i)$. Une coupe contenant l'EB_i sera donc, dans tous les cas, gardé si $P(CM_j/EB_i) \geq S_{pot} = S_p$.

Supposons maintenant que la coupe j ne contienne pas l'EB_i. Avec l'approche "manuelle", une coupe de référence CM_j est gardée si $P(CM_j) \geq S_p$. Avec un processus de troncation double cette même coupe est gardée si sa probabilité potentielle est supérieure à S_{pot}. La probabilité potentielle d'occurrence d'une coupe est toujours supérieure à sa probabilité de référence, donc, une coupe j sera dans tous les cas gardée si $P(CM_j) \geq S_{pot} = S_p$.

Avec un processus de troncation double, lorsque $S_{pot} = S_p$ et lorsque $S_{p,A} = 1$, $R_{1,i}$ sera calculé à partir du même jeu de coupes que celui issu d'un modèle dédié (approche "manuelle")

ainsi que d'autres coupes. Ces autres coupes correspondent aux coupes dont la probabilité potentielle est supérieure à S_{pot} et pour lesquelles $P\left(CM_j/EB_i\right) \leq S_{pot}$.

Si $S_{pot} = S_p$, le calcul de $R_{1,i}$ est donc plus précis quand il est issu d'un jeu de coupes de référence tronqué avec un processus double que quand il est directement calculé "à la main" au moyen d'un modèle EPS dédié.

Choix des valeurs de S_{pot} et $S_{p,A}$ utilisées dans notre processus de troncation double

Le choix de la valeur de $S_{p,A}$ ne pose pas problème. Dans la mesure où elle doit être choisie pour contrôler l'incertitude sur le risque de référence R due à la troncation du jeu de coupes, il suffit de reprendre la valeur communément utilisée pour le calcul du risque de référence (souvent 10^{-12}).

Le choix de la valeur numérique de S_{pot} est moins évident. La solution la plus simple est de choisir S_{pot} égal à $S_{p,A}$. Dans ce cas, comme on l'a vu au paragraphe précédent, l'incertitude due à la troncation du jeu de coupes est inférieure à celle résultant d'un calcul "à la main" où un jeu de coupes spécifique issu d'un modèle dédié est généré pour le calcul de chaque $R_{1,i}$.

Puisque le calcul "manuel" de l'importance des EB garantit une bonne précision des mesures d'importance, ce choix de la valeur de S_{pot} semble pertinent. Toutefois, avec cette valeur, le seuil portant sur la probabilité potentielle des coupes peut ne pas être un critère assez discriminant et le jeu de coupes en résultant peut être d'une taille encore trop importante. Dans ce cas, nous proposons de choisir la valeur de S_{pot} au moyen d'une démarche itérative semblable à celle mise en œuvre pour le calcul de la valeur du seuil probabiliste dans la section précédente (section 2.1.1 du chapitre 2 page 65).

Les valeurs de $S_{p,A}$ et de S_{pot} sont alors choisies au moyen de la démarche suivante :

1. La valeur du seuil de troncature S_{pot} est diminuée pas à pas (S_{pot_k} correspond à la valeur de S_{pot} à la $k^{\text{ème}}$ itération). Quand l'augmentation de la valeur de $\sum_{i=1}^{n} R_{1,i}$ calculée avec le seuil S_{pot_k} et le seuil $S_{pot_{k+1}}$ devient négligeable, S_{pot_k} est considérée comme une valeur acceptable du seuil pour le calcul des $R_{1,i}$.

2. La même démarche est effectuée pour le risque de référence. Quand l'augmentation de la valeur de R entre $R_{S_{p,A_j}}$ calculé avec le seuil S_{p,A_j} et $R_{S_{p,A_{j+1}}}$ calculé avec le seuil $S_{p,A_{j+1}}$ devient négligeable, S_{p,A_j} est considéré comme acceptable pour le calcul du risque de référence.

3. la plus petite valeur entre S_{pot_k} et S_{p,A_j} est sélectionnée comme seuil de troncature acceptable pour le calcul des facteurs d'importance.

Conclusion

La démarche de troncation du jeu de coupes de référence que nous proposons permet bien de garder à la fois les coupes significatives mais aussi les coupes potentiellement significatives. On contrôle alors l'incertitude due à la troncation à la fois pour le risque de référence et pour $R_{0,i}$, quel que soit i, mais aussi pour $R_{1,i}$. Le jeu de coupes de référence résultant de notre processus de troncation double est alors un jeu de coupes polyvalent qui permet à la fois le calcul précis du risque de référence mais aussi celui de toutes les mesures d'importance calculées au niveau de chaque événement de base.

Il reste donc à vérifier que notre démarche de troncation du jeu de coupes permet, à niveau de précision des facteurs d'importance égal, de les calculer à partir d'un jeu de coupes significativement plus restreint que le jeu de coupes de référence obtenu à partir d'une troncation probabiliste simple.

2.1.3 Efficacité de ce nouveau processus

Pour vérifier que notre approche a atteint son objectif, il faut donc vérifier qu'elle permet de calculer des mesures d'importance aussi précises que lorsqu'elles sont calculées au moyen du jeu de coupes de référence issu d'une troncation probabiliste simple ayant un seuil ajusté au besoin (la valeur du seuil peut être issue de la démarche de choix proposée dans la précédente section).

Comme nous allons le voir dans cette section, notre troncation probabiliste double à une efficacité fonction de la probabilité de l'EB étudié. Il faut donc vérifier de manière globale sur un exemple de taille réelle l'efficacité de ce processus de troncation.

Une efficacité fonction de la probabilité d'occurrence de l'événement de base étudié

La sous-estimation de la valeur de $R_{1,i}$ due à la troncation du jeu de coupes de référence dépend de la valeur du seuil de troncature S_p appliqué pour tronquer ce jeu de coupes, mais elle dépend aussi largement de la probabilité d'occurrence de EB_i. L'efficacité de notre processus de troncation double est tout d'abord étudiée au moyen de deux événements : "la défaillance en fonctionnement de la pompe 1" et "la défaillance à la sollicitation de la pompe 1". Ces deux événements ont un impact fonctionnel voisin (leur occurrence entraîne le même accroissement de risque) et ne diffèrent que par leur probabilité d'occurrence.

Pour un événement de base avec une forte probabilité d'occurrence : Avec un processus de troncation probabiliste simple, une coupe de référence n'est pas supprimée si sa probabilité de référence est supérieure à S_p. Avec un EB ayant une forte probabilité d'occurrence (par exemple $> 10^{-3}$), si $R_{1,i}$ est significativement différent de R, alors il y a une ou plusieurs coupes de référence contenant EB_i (notées $CM_{j,\in EB_i}$) qui deviennent dominantes lorsque cet EB est considéré comme réalisé. Si certaines $CM_{j,\in EB_i}$ deviennent dominantes lorsque EB_i est certain et puisque la probabilité d'occurrence de EB_i est élevée, alors la probabilité de référence de ces coupes est elle aussi élevée. C'est pourquoi S_p n'a pas besoin d'être très petit pour que ces coupes soient conservées. De ce fait, le seuil de troncature probabiliste simple S_{p_i} permettant un calcul peu sous-estimé de $R_{1,i}$ est relativement élevé. Le jeu de coupes de référence supérieures à S_{p_i} qui permet un calcul précis de $R_{1,i}$ est donc relativement restreint.

Avec notre processus de troncation double, les coupes ayant une forte probabilité potentielle ne sont pas supprimées. Avec un EB ayant une forte probabilité d'occurrence, si $R_{1,i}$ est significativement différent de R, alors, il y a une ou plusieurs $CM_{j,\in EB_i}$ qui ont une forte probabilité potentielle. Ces coupes seront conservées lors de la troncation double du jeu de coupes mais le jeu de coupes de référence les incluant sera plus conséquent que celui obtenu avec S_{p_i}. En effet, il contiendra à la fois des coupes dont la probabilité de référence est significative, comme dans le cas d'un processus de troncation probabiliste simple, mais aussi des coupes dont la probabilité potentielle est élevée mais dont la probabilité de référence est inférieure à S_{p_i}.

Exemple : Dans la figure 2.5, la valeur $R_{1,i}$ est exprimée en fonction de la taille du jeu de coupes à partir duquel elle est calculée lorsque ce jeu de coupes est issu d'un processus de troncation simple et lorsqu'il est issu de notre processus de troncation double (avec $S_{p,A} = 1$). L'EB_i correspond à l'événement "défaillance en fonctionnement de la pompe 1" et a une probabilité d'occurrence de $2,2 \cdot 10^{-3}$.

Cet exemple souligne le fait que, pour des EB ayant une probabilité d'occurrence élevée, et à taille de jeu de coupes égale, l'incertitude due à la troncation du jeu de coupes est légèrement plus faible avec une troncation probabiliste simple qu'avec notre processus double. Toutefois, notre approche converge rapidement vers l'approche probabiliste simple.

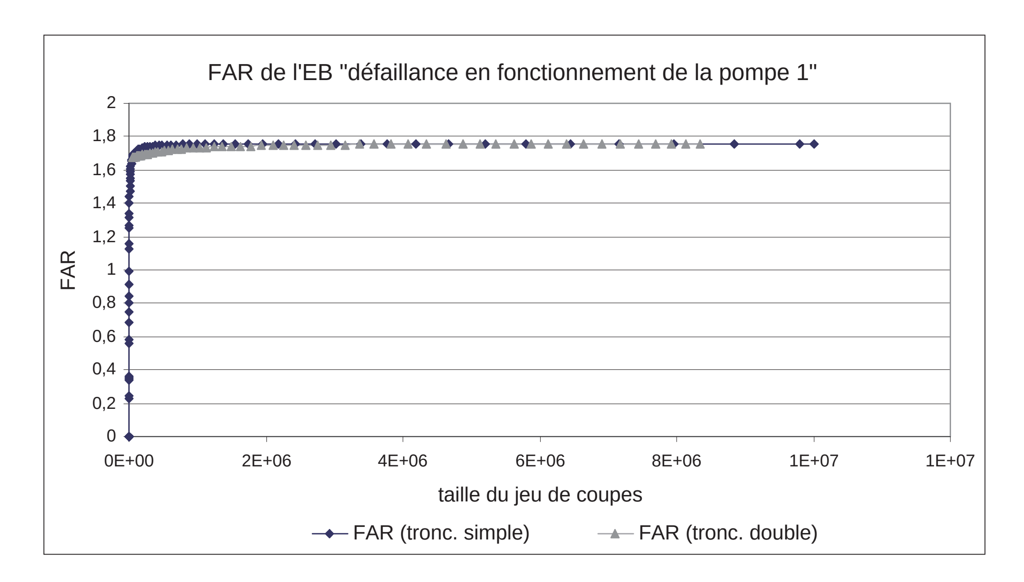


Fig. 2.5 – *Évolution du FAR en fonction de la taille du jeu de coupes utilisé pour un EB dont la probabilité d'occurrence est "grande"*

Pour un événement de base avec une faible probabilité d'occurrence : Avec un processus de troncation probabiliste simple, une coupe de référence n'est pas supprimée si sa probabilité de référence est supérieure à S_p. Avec un EB ayant une faible probabilité d'occurrence (par exemple $< 10^{-5}$), si $R_{1,i}$ est significativement différent de R, alors il y a une ou plusieurs coupes de référence contenant EB_i qui deviennent dominantes lorsque cet EB est considéré comme étant certain. Si certaines $CM_{j,\in EB_i}$ deviennent dominantes lorsque EB_i est certain, cela implique que pour ces coupes, $P\left(CM_{j,\in EB_i}\right)/P\left(EB_i\right)$ est significatif mais puisque $P\left(EB_i\right)$ est faible, la probabilité de ces coupes dans le cadre du risque de référence $\left(P\left(CM_{j,\in EB_i}\right)\right)$ peut être très faible. C'est pourquoi S_p doit être très petit pour que ces coupes soient conservées. De ce fait, le seuil de troncature probabiliste simple S_{p_i} permettant un calcul peu sous-estimé de $R_{1,i}$ est relativement petit. Le jeu de coupes de référence supérieures à S_{p_i} qui permet un calcul précis de $R_{1,i}$ est donc volumineux.

Avec notre processus de troncation double, les coupes ayant une forte probabilité potentielle ne sont pas supprimées. Si $R_{1,i}$ est significativement différent de R, alors, il y a une ou plusieurs $CM_{j,\in EB_i}$ qui ont une forte probabilité potentielle. Ces coupes seront conservées lors de la troncation double du jeu avec un seuil S_{pot} relativement élevé, et ce, quelle que soit la probabilité d'occurrence de EB_i.

Avec un processus de troncation double, un jeu de coupes de référence beaucoup plus compact permettra le calcul peu sous-estimé de $R_{1,i}$ lorsque EB_i a une probabilité d'occurrence faible.

Exemple : Dans la figure 2.6, la valeur $R_{1,i}$ est exprimé en fonction de la taille du jeu de coupes à partir duquel elle est calculée lorsque ce jeu de coupes est issu d'un processus de troncation simple et lorsqu'il est issu de notre processus de troncation double (avec $S_{p,A} = 1$). L'EB_i correspond à l'événement "rupture de la pompe 1" et a une probabilité d'occurrence de $7,2 \cdot 10^{-8}$.

Cet exemple illustre le fait que notre approche est significativement plus efficace qu'une troncation probabiliste simple pour les EB ayant une faible probabilité d'occurrence. Ainsi, pour atteindre la valeur asymptotique de $R_{1,i}$, 1 880 000 coupes sont nécessaires avec notre approche alors qu'une approche basée sur une troncation probabiliste simple nécessite plus de

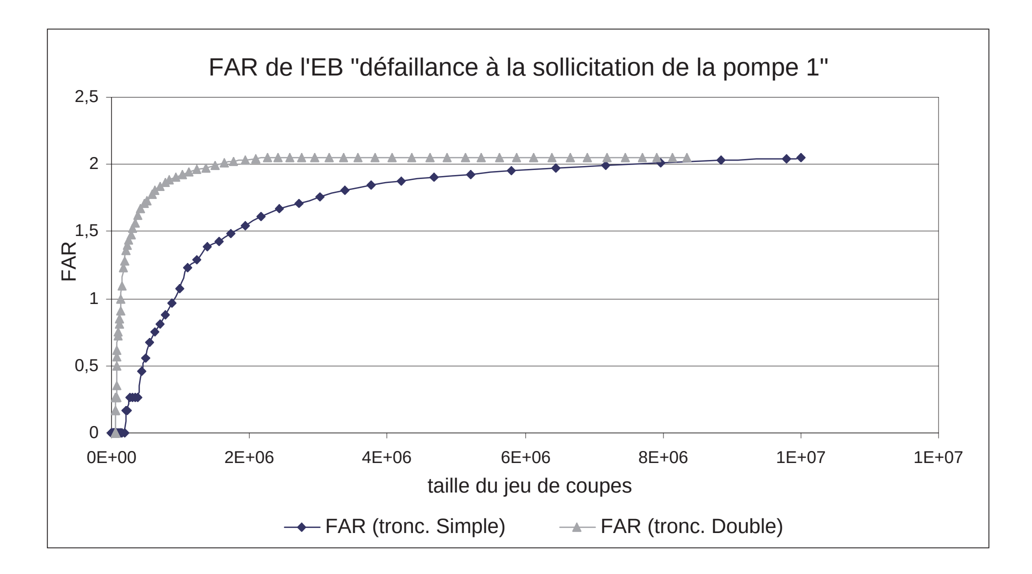


FIG. 2.6 – *Évolution du FAR en fonction de la taille du jeu de coupes utilisé pour un EB dont la probabilité d'occurrence est "faible"*

8 000 000 coupes.

Vérification globale

Si, pour les EB peu probables, notre processus de troncation double semble plus efficace alors que pour les EB probables, il semble être équivalent à une troncation probabiliste simple, l'amélioration apportée par notre processus de troncation doit être démontrée de manière globale.

Plutôt que de démontrer sur un plan théorique la supériorité de notre processus de troncation double sur un processus de troncation simple pour générer un jeu de coupes de référence permettant le calcul des facteurs d'importance, nous avons préféré vérifier son efficacité sur les modèles EPS réels d'EDF. Ainsi, toutes les figures présentées dans la suite de cette section correspondent au modèle EPS de niveau 1 des centrales 900MWe d'EDF. Les résultats obtenus sur les modèles des centrales 1300MWe et EPR sont sensiblement identiques.

Méthode employée : L'objectif de notre travail était de réduire la taille du jeu de coupes de référence permettant de calculer l'importance des EB sans qu'elles soient sous-estimées du fait de la troncation du jeu de coupes. Donc, pour s'assurer que notre méthode a bien atteint ses objectifs, la vérification suivante a été effectuée :

1. Les valeurs de $R_{1,i}$ ont été calculées, pour chaque EB, à partir d'un jeu de coupes issu d'une troncation probabiliste simple pour différentes valeurs de S_p comprises entre 10^{-12} et 10^{-25}. Le nombre de coupes de références générées pour chaque valeur de S_p est noté.
2. Les valeurs de $R_{1,i}$ ont été calculées pour chaque EB, à partir d'un jeu de coupes issu d'une troncation probabiliste double pour différentes valeurs de S_{pot} comprises entre 10^{-4} et 10^{-23} et pour $S_{p,A} = 10^{-12}$. Le nombre de coupes de références générées pour chaque valeur de S_{pot} est noté.
3. Pour différents pourcentages d'incertitude [5] sur $R_{1,i}$ (1%, 5%, 10%, 15% et 20%), la taille de jeu de coupes nécessaires pour que cette incertitude maximum ne soit pas dépassée

[5] Le pourcentage d'incertitude est défini à partir de la valeur des $R_{1,i}$ estimée lorsque $S_p = 10^{-25}$:
$$\% \text{ incertitude au seuil } S_p = 10^{-x} = \frac{R_{1,i}|_{S_p=10^{-25}} - R_{1,i}|_{S_p=10^{-x}}}{R_{1,i}|_{S_p=10^{-25}}}$$

dans le pire des cas (l'EB nécessitant le plus grand jeu de coupes pour ne pas dépasser ce degré d'incertitude) est définie.

On ne considérera que les EB contenus dans des coupes potentiellement significatives (on ne s'intéresse pas aux EB non-importants quel que soit le seuil). En effet, pour un EB dont l'importance est négligeable, on pourra accepter que ses mesures d'importance soient imprécises. Pour ce faire, on ne prendra en compte que les EB dont le FAR est supérieur à une certaine valeur.

Résultats et commentaires : La figure 2.7 présente les résultats de cette vérification lorsque seuls les EB dont le FAR est supérieur à 0,5 sont considérés. Il est alors évident que notre approche permet de diminuer la taille du jeu de coupes de 70 à 90 pour cent.

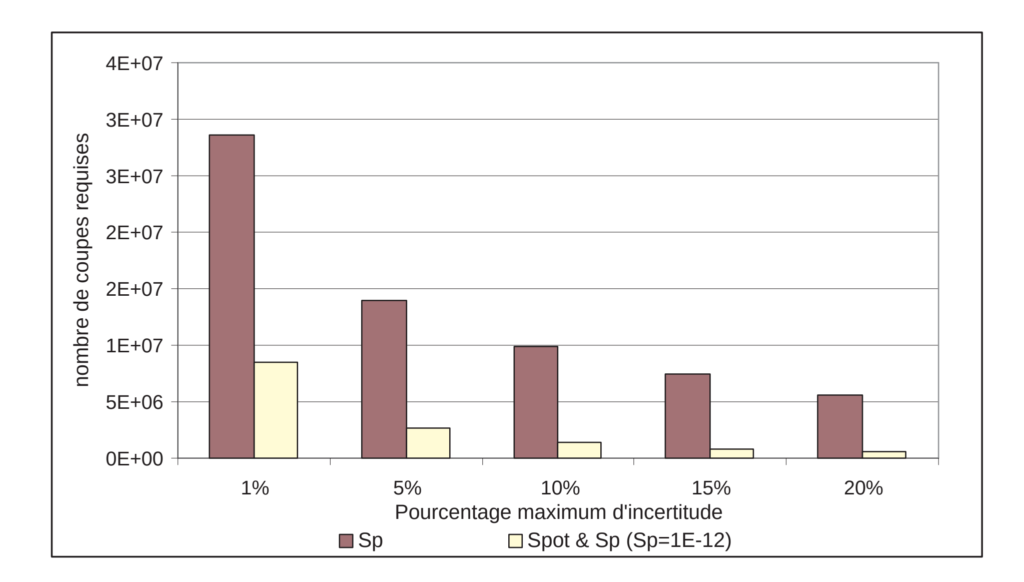


FIG. 2.7 – *Taille du jeu de coupes requis pour atteindre le niveau de précision sur $R_{1,i}$ demandé pour les EB dont le FAR est plus grand que 0,5*

L'efficacité de notre approche doit aussi être testée lorsque davantage d'EB sont considérés. On génère donc la figure 2.8, qui présente les résultats de cette vérification lorsque seuls les EB dont le FAR est supérieur à 0,1 sont considérés.

La figure 2.8 peut surprendre en ce que la taille du jeu de coupes issu d'une troncation probabiliste simple est toujours la même, quelle que soit la précision demandée sur les $R_{1,i}$. Cela s'explique par le fait qu'un EB ayant une probabilité d'occurrence très faible (10^{-20}) voit sa valeur de $R_{1,i}$ passer de 0 à $1,32$ fois le risque de référence quand le seuil de troncature est plus petit que $1,26 \cdot 10^{-25}$. Donc, toutes les coupes dont la probabilité est supérieure à $1,26 \cdot 10^{-25}$ sont nécessaires pour atteindre une précision de 1%, 5%, 10%, 15% ou 20% sur la valeur de $R_{1,i}$ pour cet EB.

Conclusion

L'objectif de notre approche est de calculer à partir d'un seul jeu de coupes de référence, le plus compact possible, toutes les mesures d'importance sans qu'elles soient significativement sous-estimées du fait de la troncation de ce jeu de coupes.

Au vu des résultats obtenus avec les modèles EPS d'EDF, on peut considérer cet objectif comme atteint. En effet, lorsque notre processus de troncation probabiliste double est comparé à un processus de troncation probabiliste simple, on se rend compte que, pour atteindre le même niveau de précision sur les mesures d'importance, un jeu de coupes beaucoup moins important

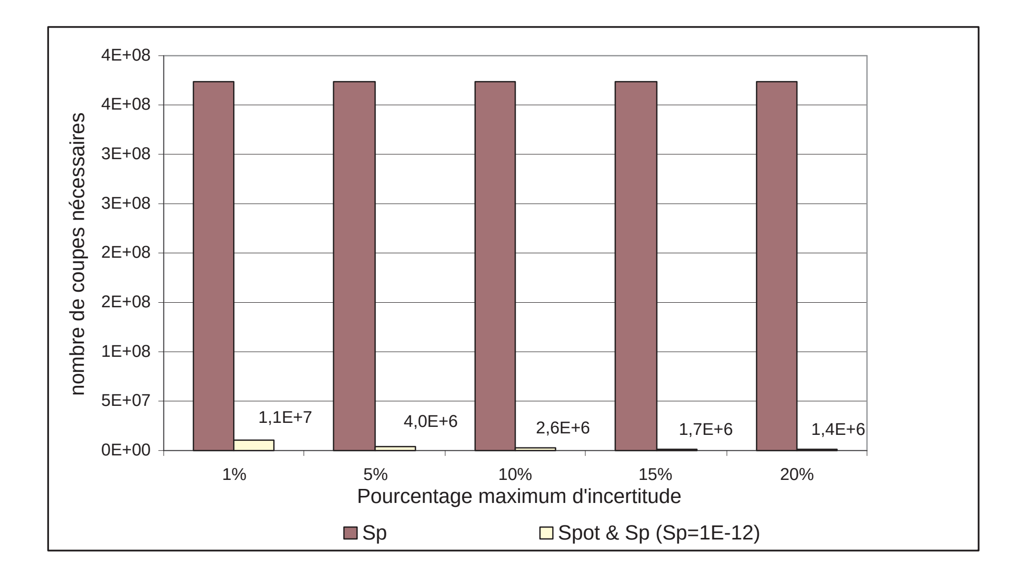


FIG. 2.8 – *Taille du jeu de coupes requis pour atteindre le niveau de précision sur $R_{1,i}$ demandé pour les EB dont le FAR est plus grand que 0,1*

est nécessaire.

Le fait d'utiliser un jeu de coupes beaucoup plus compact permet de rester dans les limites des matériels informatiques supportant les modèles mais cela permet aussi de réduire de manière notable les temps de calcul des mesures d'importance.

2.2 Automatisation du calcul des facteurs d'importance : l'application SENSIB

Comme on l'a vu dans la première partie de ce chapitre, l'objectif en matière de facteurs d'importance est de permettre leur calcul précis, rapide, simple et sûr (pas de risque d'erreur). Le nouveau processus de troncation probabiliste double que nous venons de présenter permet d'améliorer la précision et la rapidité de calcul des mesures d'importance. Toutefois, il reste à le mettre en œuvre et à améliorer la simplicité et la "sécurité" du calcul des facteurs d'importance.

A cette fin, nous avons développé le prototype d'une application informatique pilotant la production des coupes de RSW et post-traitant celles-ci pour calculer les mesures d'importance. Dans cette section, la nature du besoin, les principales fonctionnalités et les avancées méthodologiques associées à cette application sont présentées.

2.2.1 Nature du besoin

RSW propose, en même temps qu'il génère les coupes minimales, de calculer automatiquement les principales mesures d'importance de chaque EB. Ce calcul automatique a pourtant plusieurs limites qui méritent d'être levées.

Ainsi, plusieurs constats nous ont poussés à développer une nouvelle application informatique autour de RSW :

1. On ne peut pas, avec RSW, générer plus de 10 millions de coupes en une seule fois. Les mesures d'importance automatiquement calculées par RSW sont donc calculées avec un jeu de coupes de référence issu d'une troncation probabiliste simple et contenant au mieux 10 millions de coupes. Pourtant, l'étude de l'impact de la troncation probabiliste simple d'un jeu de coupes de référence montre que 10 millions de coupes ne suffisent pas

pour calculer, sans les sous-estimer, toutes les mesures d'importance de tous les EB. La valeur $R_{1,i}$, pour les EB ayant une faible probabilité d'occurrence, est trop imprécise et difficilement majorable.

2. Lorsque RSW calcule automatiquement les $R_{1,i}$ à partir des coupes de référence, il ne supprime pas les coupes devenues non-minimales lorsque EB_i est certain (c.f. section 4.2.4 du chapitre 1).
3. Les mesures d'importance automatiquement calculées par RSW à partir des coupes minimales sont des valeurs numériques données sans aucun intervalle de confiance ni toute autre indication de la qualité d'estimation de ces valeurs (on ne connaît en particulier pas l'impact de la troncation du jeu de coupes de référence).
4. Les mesures d'importance intégrant les défaillances de cause commune ne sont pas prises en compte par RSW et doivent être calculées à la main. Ainsi, on ne peut pas connaître automatiquement l'importance de la défaillance de la pompe 1 toutes causes confondues (DCC ou intrinsèque).
5. Lorsque l'on effectue des études de sensibilité du risque à des modifications, un ou plusieurs EB sont considérés comme réalisés et certaines probabilités d'occurrence de certains EB sont modifiées. Ces modifications peuvent être intégrées au modèle EPS de référence pour obtenir un modèle dédié à cette étude. RSW produira dans ce cas un jeu de coupes dédié correspondant au risque sachant ces modifications. Il est alors difficile de savoir quelles coupes de référence sont modifiées lorsque ces événements sont certains ou lorsque ces probabilités sont modifiées. La correspondance entre les coupes de référence et les coupes dédiées n'est pas facile à faire : il est difficile de savoir, pour certaines coupes dédiées, à quelles coupes de référence elles correspondent.

L'objectif que nous nous sommes fixé est donc de répondre à ces divers manques par une seule application appelée ici SENSIB. Tout en gardant comme outil central RSW, celle-ci doit pallier à ses limites.

2.2.2 Calculer automatiquement les mesures d'importance à partir des bonnes données

RSW ne peut pas générer plus de 10 millions de coupes en un seul calcul et un tel jeu de coupes ne permet pas un calcul des mesures d'importance sans biais dû à cette troncation, comme le montre l'annexe C. Pour avoir un jeu de coupes plus conséquent, il faut pouvoir fractionner la génération des coupes de référence. C'est un préalable à tout calcul de mesures d'importance basé sur les coupes de référence. L'objectif de cette section est donc de présenter notre démarche de construction du jeu de coupes de référence et de calcul des valeurs $R_{1,i}$ et $R_{0,i}$ pour chaque EB.

En s'inspirant de la méthode proposée par Balmain dans [9], on peut générer un jeu de 10 millions de coupes pour chaque initiateur et fusionner ensuite ces jeux de coupes pour obtenir le jeu de coupes de référence. En effet, dans les modèles EPS d'EDF, l'hypothèse est faite que les événements initiateurs sont exclusifs (deux événements initiateurs de deux arbres d'événements différents ne peuvent pas se produire simultanément). Un jeu de coupes de référence correspond donc à la réunion des jeux de coupes correspondant à chaque arbre d'événement.

A partir de ce principe de découpage de la création du jeu de coupes par arbre d'événements, on peut mettre au point le processus de génération automatique des coupes de référence suivant :

1. j correspond à l'indice de l'arbre d'événements étudié. On initialise j à 1 pour commencer par le premier arbre d'événements de l'EPS considérée.
2. L'application SENSIB pilote RSW pour générer les dix premiers millions de coupes de l'arbre d'événements j (ou toutes ses coupes si cet arbre d'événements correspond à moins

de 10 millions de coupes). RSW génère automatiquement un fichier de résultats contenant ces coupes. On garde en mémoire le seuil $S_{pN,j}$ correspondant à la plus basse probabilité des coupes générées (dans l'arbre d'événements j, en-dessous de $S_{pN,j}$, les coupes ont été supprimées et au-dessus, elles ont été conservées).

3. Notre application lit ce fichier de résultat. Lors de la lecture de ces coupes, elle met à jour l'ensemble des valeurs des $R_{0,i}$ et des $R_{1,i}$ en conservant les coupes non-minimales lorsque EB_i est considéré comme certain.

   Lors de cette même lecture, elle sélectionne les coupes significatives ou potentiellement significatives à partir du processus de troncation double présenté dans la section 2.1.3 page 71 de ce chapitre. Elle enregistre les coupes sélectionnées. Elle met à jour la valeur de $\Delta_{TRM,j}$ (qui correspond au majorant de l'erreur commise sur le calcul de R_j, qui est le risque de référence en ne considérant que l'arbre d'événements j) en ajoutant à cette valeur, issue de RSW, la probabilité des coupes tronquées par ce processus de troncation double.

4. Elle supprime le fichier de résultats issu de RSW et correspondant à l'arbre d'événements j pour dégager de l'espace mémoire.

5. Elle considère l'arbre suivant en recommençant au point 2 de ce processus avec ce nouvel arbre. Cela signifie que $j = j + 1$, à moins que le dernier arbre d'événements n'ait déjà été considéré. Dans ce cas, le processus s'arrête.

Suite à l'exécution de ce processus, on dispose donc :
- de la valeur du risque de référence R, qui est égale à la somme des R_j.
- de toutes les valeurs des $R_{0,i}$,
- de toutes les valeurs des $R_{1,i}$ calculées à partir de jeux de coupes contenant des coupes non-minimales (les coupes de référence devenant non-minimales lorsque EB_i est certain),
- d'un jeu de coupes de référence relativement compact, issu d'une troncation double, qui permettra, pour chaque EB_i, d'identifier les coupes non-minimales lorsque cet EB est certain. On pourra alors calculer la valeur considérée comme sans biais de chaque $R_{1,i}$ comme étant la valeur précédemment calculée moins la probabilité d'occurrence de l'union des coupes non-minimales lorsque EB_i est certain,
- d'un majorant de l'erreur due à sa troncation, qui est Δ_{TRM} (égal à la somme des $\Delta_{TRM,j}$).

On sait, de plus, que les $R_{1,i}$ ont été calculés à partir d'un jeu de coupes contenant toutes les coupes supérieures au plus grand des $S_{pN,j}$. On appelle cette valeur $S_{p,N_{init}}$. Elle correspond au seuil de troncature le plus petit possible lorsqu'on génère les coupes de référence par initiateur avec RSW.

$$S_{p,N_{init}} = \max_j [S_{p,N,j}]$$

Même si on dispose aussi de certaines coupes dont la probabilité est inférieure à $S_{p,N_{init}}$ (des coupes issues d'arbres d'événements où la valeur de $S_{p,N,j}$ était plus faible), on est obligé, pour être conservatif, de considérer $S_{p,N_{init}}$ comme étant le seuil de troncature du jeu de coupes de référence dont les $R_{0,i}$ et les $R_{1,i}$ sont issus.

On dispose d'une très bonne estimation de la valeur du risque de référence (elle n'est quasiment pas impactée par la troncation du jeu de coupes), et pour chaque EB , de la meilleure estimation possible, au vu des limites de RSW, de $R_{1,i}$ et de $R_{0,i}$. On peut alors calculer (ou approximer dans le cas du VF) toutes les mesures d'importance courantes.

2.2.3 *Information sur la sous-estimation des mesures d'importance due à la troncation*

Bien que le processus de génération mis en œuvre par notre application vise à avoir le jeu de coupes le plus complet possible, il peut ne pas être suffisant pour bien calculer l'importance d'EB ayant une exceptionnellement faible probabilité d'occurrence (10^{-20} par exemple). En

effet, il faut garder à l'esprit que les coupes qui sont utilisées pour calculer les $R_{1,i}$ et les $R_{0,i}$ sont obtenues grâce à une troncation probabiliste simple appliquée à chaque arbre d'événements. Ce n'est qu'ensuite qu'elles sont tronquées à nouveau grâce à une troncation probabiliste double. Il ne s'agit donc pas d'une vraie troncation probabiliste double qui lèverait toutes incertitudes significatives due à la troncation du jeu de coupes. De plus, le seuil de troncature des coupes de référence employé dans cette troncation probabiliste simple n'a pas été choisi mais subi. En effet, comme on l'a vu dans la section précédente, la valeur de la probabilité de la première coupe tronquée ($S_{p,N_{init}}$) dépend de la structure du modèle.

Il faut donc vérifier pour chaque EB_k que le jeu de coupes utilisé pour calculer son importance est suffisant.

Comment juger de l'ampleur la sous-estimation de l'importance des EB

Principe : Dans la mesure où le risque de référence R converge rapidement lorsqu'il est calculé à partir de peu de coupes (c.f. figure 1.16 page 54 du chapitre 1) et dans la mesure où, dans notre cas, R est calculé à partir de plusieurs fois 10 millions de coupes, on ne considérera que la sous-estimation des $R_{1,i}$.

Pour juger de l'ampleur de leur sous-estimation, deux types d'informations sont utilisés :
- la somme des $R_{1,i}$ des EB_i ayant une probabilité d'occurrence comprise dans la même décade que l'EB_k étudié (: si $P(EB_k) = 2,3 \cdot 10^{-5}$ on considérera la somme des $R_{1,i}$ des EB_i ayant une probabilité d'occurrence comprise entre 10^{-4} et 10^{-5}),
- la probabilité de la première coupe tronquée contenant l'EB_k quand EB_k est considéré comme certain dans le pire des cas. Cette probabilité, notée $P_{T,pc,/k}$, est calculée à partir de la probabilité de la première coupe tronquée ($S_{p,N_{init}}$) lors de la génération du jeu de coupes.

$$P_{T,pc,/k} = \frac{S_{p,N_{init}}}{P(EB_k)}$$

On considère alors que la valeur de $R_{1,k}$ n'est pas trop sous-estimée si cette somme semble converger et si la valeur de $R_{1,k}$ est plusieurs dizaines de fois plus grande que celle de $P_{T,pc,/k}$ (par exemple, $\frac{R_{1,k}}{P_{T,pc,/k}} > 10^6$)

Justification : Une très bonne estimation de la valeur du risque de référence est obtenue en ne considérant que les coupes dont la probabilité d'occurrence est supérieure à $R \cdot 10^{-6}$. Par analogie, nous supposons qu'une valeur sans biais de $R_{1,i}$ est obtenue lorsque toutes les coupes sachant EB_i dont la probabilité est supérieure à $R_{1,i} \cdot 10^{-6}$ sont conservées. Cela équivaut à dire que $\frac{R_{1,i}}{P_{T,pc,/k}} > 10^6$.

Pour savoir si la valeur des $R_{1,i}$ converge pour un seuil de troncature donné (i.e. si pour ce seuil l'impact de la troncation est nul), on regarde l'évolution de la somme des $R_{1,i}$ en fonction du seuil. Lorsqu'un $R_{1,i}$ est calculé à partir des coupes de référence, l'importance de cette sous-estimation est proportionnelle à la probabilité d'occurrence de EB_i. Il peut donc paraître logique de chercher, pour un seuil de troncature donné, si la valeur de $R_{1,i}$ des EB dont la probabilité d'occurrence est comprise entre 1 et 10^{-1} converge, puis si c'est le cas, si celles des EB dont la probabilité d'occurrence est comprise entre 10^{-1} et 10^{-2} convergent, et ainsi de suite.

Mise en œuvre de cette démarche : Pour indiquer l'ampleur de la sous-estimation de l'importance de chaque EB, nous avons défini quatre niveaux :

Vert	La précision de la valeur calculée est bonne
Jaune	La valeur calculée peut être légèrement sous-estimée
Orange	La valeur calculée ne donne qu'un ordre de grandeur et peut être fortement sous-estimée
Rouge	la valeur calculée n'a aucun sens, elle peut être très fortement sous-estimée

TAB. 2.1 – *Code de couleur indiquant la précision des facteurs d'importance calculés*

Chacun de ces niveaux correspond à des critères portant sur la valeur de $R_{1,i}$. Ainsi l'incertitude d'un facteur d'importance de EB_k dont la formule contient $R_{1,k}$ sera caractérisée de la manière suivante :

1. Il sera vert si :
   - la somme des $R_{1,i}$ des EB dont la probabilité d'occurrence appartient à la même décade que celle de EB_k, exprimée en fonction du seuil de troncature, a atteint son asymptote avant la valeur $S_{p,N_{init}}$,
   - $R_{1,i} \cdot 10^{-6} > P_{T,pc,/k}$ OU $P_{T,pc,/k} < 10^{-12}$
2. Il sera jaune s'il n'est pas vert et si :$R_{1,i} \cdot 10^{-6} > P_{T,pc,/k}$ OU $P_{T,pc,/k} < 10^{-12}$
3. Il sera orange s'il n'est ni vert ni jaune et si : $R_{1,i} \cdot 10^{-5} > P_{T,pc,/k}$ OU $P_{T,pc,/k} < 10^{-10}$.
4. s'il ne valide aucun de ces critères, il sera rouge.

Les facteurs d'importance dont la formule ne contient que $R_{0,k}$ et R seront verts si : $S_{p,N_{init}} < 10^{-15}$.
Ils seront oranges si : $S_{p,N_{init}} < 10^{-12}$ et rouges sinon.

2.2.4 Fonctionnalités de SENSIB

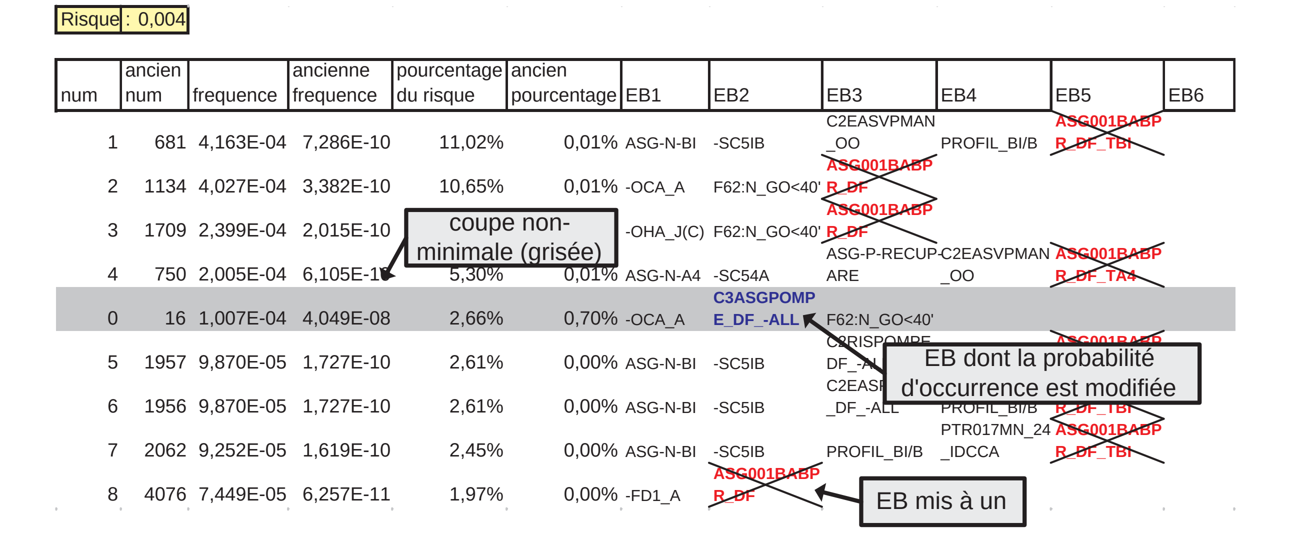
L'application que nous avons développée calcule, à partir du jeu de coupes qu'elle a généré, les différentes mesures d'importance pour chaque EB. Les différences majeures avec les mesures d'importance proposées par RSW sont les suivantes :

1. Lorsque les $R_{1,i}$ sont calculés automatiquement, les coupes non-minimales, lorsque EB_i est certain, sont bien supprimées dans ce calcul. Il n'y a donc pas de surestimation de $R_{1,i}$ due aux coupes non-minimales.
2. Lorsque plusieurs EB modélisent le même événement de base dont la probabilité d'occurrence est définie à partir de plusieurs temps de mission, notre application peut calculer l'importance d'un unique événement, tous temps de mission confondus.
3. Lorsqu'un EB appartient à un groupe DCC, notre application peut calculer l'importance de cet événement toutes causes confondues (défaillance intrinsèque et défaillances de cause commune).
4. Comme RSW, notre application permet d'effectuer des analyses de sensibilité. Mais, contrairement à RSW qui ne présente que le jeu de coupes correspondant au risque sachant les modifications correspondant à l'analyse (EB considérés comme réalisés, probabilités d'occurrence modifiées etc.), elle explicite les modifications du jeu de coupes de référence pour arriver à celui correspondant à l'analyse de sensibilité. Ainsi, pour chaque coupe, on peut connaître :
   - si elle est toujours minimale,
   - sa probabilité dans le cadre du risque de référence et sa probabilité dans le cadre de l'analyse de sensibilité,
   - l'ordre de la coupe dans le classement par ordre de probabilité décroissante dans le jeu de coupes de référence et dans le jeu de coupes dédié à l'analyse de sensibilité,

- le ou les EB mis à 1, contenus dans cette coupe,
- le ou les EB dont la probabilité d'occurrence a été modifiée par rapport à leur probabilité d'occurrence de référence,
- la contribution de la coupe dans le cadre du risque de référence et lorsque l'événement PGT est certain.

Ces résultats sont alors exportés sous Excel pour pouvoir être mis en forme.

Exemple : La figure 2.9 présente les premières coupes issues du modèle EPS des tranches 900MWe d'EDF lorsque la probabilité d'occurrence de l'EB "`ASG002POMPE_DF` est deux fois supérieure à la normale et lorsque l'EB "`ASG001TCVAP_SC`" est considéré comme certain.



Risque : 0,004

num	ancien num	frequence	ancienne frequence	pourcentage du risque	ancien pourcentage	EB1	EB2	EB3	EB4	EB5	EB6
1	681	4,163E-04	7,286E-10	11,02%	0,01%	ASG-N-BI	-SC5IB	C2EASVPMAN_OO	PROFIL_BI/B	~~ASG001BABPR_DF_TBI~~	
2	1134	4,027E-04	3,382E-10	10,65%	0,01%	-OCA_A	F62:N_GO<40'	~~ASG001BABPR_DF~~			
3	1709	2,399E-04	2,015E-10	[illegible]	[illegible]	-OHA_J(C)	F62:N_GO<40'	~~ASG001BABPR_DF~~			
4	750	2,005E-04	6,105E-1[illegible]	5,30%	0,01%	ASG-N-A4	-SC54A	ASG-P-RECUPARE	C2EASVPMAN_OO	~~ASG001BABPR_DF_TA4~~	
0	16	1,007E-04	4,049E-08	2,66%	0,70%	-OCA_A	C3ASGPOMPE_DF_-ALL	F62:N_GO<40'			
5	1957	9,870E-05	1,727E-10	2,61%	0,00%	ASG-N-BI	-SC5IB	C2RISPOMPEDF_-AL[illegible]	[illegible]	[illegible]	
6	1956	9,870E-05	1,727E-10	2,61%	0,00%	ASG-N-BI	-SC5IB	C2EAS[illegible]_DF_-ALL	PROFIL_BI/B	~~R_DF_TBI~~	
7	2062	9,252E-05	1,619E-10	2,45%	0,00%	ASG-N-BI	-SC5IB	PROFIL_BI/B	PTR017MN_24_IDCCA	~~ASG001BABPR_DF_TBI~~	
8	4076	7,449E-05	6,257E-11	1,97%	0,00%	-FD1_A	~~ASG001BABPR_DF~~				

Fig. 2.9 – *Exemple de fichier de résultat*

Toutes ces informations permettent une bien meilleure interprétation de la modification du risque lors d'une étude de sensibilité.

5. L'importance de l'incertitude liée à la troncation du jeu de coupes est indiquée de manière qualitative. La mise en œuvre de cette estimation est détaillée dans la section précédente.

2.2.5 Conclusion sur SENSIB

Avec cette application, on dispose donc d'un outil permettant d'effectuer automatiquement le calcul le plus précis possible des mesures d'importance à partir d'un jeu de coupes de référence. De plus, le nombre d'opérations manuelles étant réduit, le risque d'erreur de calcul l'est aussi et l'importance des incertitudes liées à la troncation du jeu de coupes de référence est explicitée pour chaque mesure d'importance de chaque EB. Enfin, l'interprétation des résultats est facilitée.

3 Conclusion sur la gestion des incertitudes

La démarche de gestion des incertitudes que nous mettons en œuvre vise à la fois à minimiser les incertitudes sur les mesures d'importance et à générer un minimum de surcroît de travail lors de leur calcul. Ainsi, seules les simplifications de modélisation qui ont un trop fort impact sur les mesures d'importance ont été identifiées comme devant être corrigées. De même, le gain de

précision résultant du meilleur traitement des incertitudes liées à la troncation du jeu de coupes de référence a été obtenu sans alourdir la procédure de calcul des mesures d'importance, grâce à une complète automatisation. Bien que les modèles EPS restent une représentation simplifiée des centrales nucléaires et que les indicateurs qui en sont issus ne puissent être le seul critère pour justifier une décision, la réduction des incertitudes à laquelle nous avons abouti permet d'envisager une plus large utilisation des mesures d'importance dans des processus de décision.

Chapitre 3

Indicateurs d'importance de macro-événements

Les méthodes actuelles qui emploient les mesures d'importance considèrent principalement l'importance d'événements de base (EB) qui modélisent le plus souvent un mode de défaillance spécifique d'un matériel spécifique. Le développement de nouvelles applications basées sur des mesures d'importance peut nécessiter de calculer l'importance d'événements non élémentaires comme la défaillance d'un système ou l'importance d'une mission de sauvegarde. Avant de pouvoir développer ces nouvelles applications, il convient de définir les événements non élémentaires qui peuvent être étudiés et la signification des indicateurs relatifs à ces événements. Ensuite, l'application de ces indicateurs sera illustrée par leur mise en œuvre dans le cadre d'une démarche de gestion des cumuls d'indisponibilité.

1 Clarification sur les niveaux de calcul possibles des indicateurs de risque

1.1 Contexte et objectifs

Les facteurs d'importance sont bien définis et couramment employés dans les applications des EPS, dans des projets tels que l'optimisation de la maintenance par la fiabilité (OMF) ou l'identification des matériels sensibles.

De nos jours, le champ d'application des EPS grandit et le calcul de mesures d'importance uniquement au niveau des événements de base devient un peu trop restrictif. L'optimisation des performances sous contrainte de sûreté doit pouvoir s'appuyer sur des outils adaptés de contrôle du risque. Dans ce cadre, l'utilisation des mesures d'importance pour étudier des événements plus "complexes", tels que la défaillance d'un système ou celle d'une mission, doit pouvoir être envisagée. On parlera alors de macro-événements et non plus d'événements élémentaires.

L'extension des mesures d'importance classiques (FAR, FDR, RRW, RAW, etc.) aux macro-événements a plusieurs fois été envisagée [88, 89, 42, 94, 98, 64, 29, 27]. Toutefois, si la définition de l'importance d'un événement tel que la défaillance d'un composant fait l'objet d'un consensus, il existe plusieurs définitions de l'importance d'un système [41, 20, 88, 36] ou d'une fonction. De plus, les applications potentielles de facteurs d'importance calculés pour un système sont floues. Il nous a donc semblé utile, avant d'utiliser ces mesures d'importance classiques pour étudier des macro-événements, de les redéfinir clairement, d'en exposer la signification physique et d'en explorer les potentielles applications.

Dans ce chapitre, nous proposons une extension des mesures d'importance communément

utilisées dans les EPS pour considérer non plus des événements de base mais des macro-événements. Elles sont donc, dans la suite de ce chapitre, appelées de manière générique "mesures d'importance étendues" car elles sont étendues au-delà des événements de base.

Notre premier objectif est de présenter trois types d'événements "complexes" qui peuvent être étudiés au moyen de mesures d'importance étendues :
- l'événement "occurrence (ou non-occurrence) simultanée de plusieurs événements de base",
- l'événement "défaillance d'un système",
- la "non-existence" ou le "parfait fonctionnement" d'une fonction (par exemple, la non-existence de la fonction "injection de sûreté haute pression").

Notre second objectif est de clarifier, pour chacun de ces trois niveaux d'extension des facteurs d'importance, quelles sont leur signification et leurs applications potentielles. Pour appuyer notre propos, un même exemple sera développé afin d'illustrer les différences entre les divers niveaux pour lesquels on peut considérer ces mesures d'importance étendues.

1.2 Quels facteurs d'importance considérer pour quels macro-événements

Notre but est de calculer des facteurs d'importance d'événements qui ne sont plus des événements élémentaires (ou de base) mais des macro-événements. Nous définissons les macro-événements comme des événements qui peuvent être exprimés à partir d'événements de base, par exemple au moyen d'une fonction de structure, mais qui sont différents d'eux sur plusieurs points :
- ils ne sont pas forcément indépendants les uns des autres,
- ils dépendent de certains événements de base,
- ils ne sont pas forcément modélisés explicitement dans le modèle EPS.

Les macro-événements seront notés E par opposition aux événements de base, notés EB.

Certains facteurs d'importance probabilistes, présentés dans la section 2.1.3, ne sont définis que pour des événements de base. Ils ne pourront pas être étendus pour considérer l'importance de macro-événements. C'est le cas, par exemple, du facteur de Vesely-Fussel. On ne peut pas étendre la définition "*le Facteur de Vesely Fussel (VF) d'un événement [de base] i se définit comme la probabilité qu'une coupe contenant EB_i soit réalisée sachant que l'événement CI s'est produit*" à des macro-événements (que signifie "le macro- événement est dans la coupe" ?). On pourra toutefois considérer le FDR d'un macro-événement en lieu et place de son VF dans la mesure où, pour un EB, les deux définitions sont très proches. De même, le facteur DIM est déjà défini pour un ensemble d'événements de base et n'a plus de sens si l'on veut grâce à lui estimer l'importance d'un macro-événement. Enfin, même si l'on peut envisager l'extension du facteur de sensibilité aux macro-événements, son interprétation dans ce cas peut ne pas être aisée. Ainsi, considérer qu'un système voit sa probabilité d'occurrence varier de Δ_P peut ne pas suffire. Encore faut-il savoir quels sont les composants dont la variation de la probabilité de défaillance justifie cette variation Δ_P.

Tous les autres facteurs d'importance précédemment présentés (FAR, FDR, I_B, RRW et RAW) qui peuvent eux être étendus s'expriment uniquement en fonction de $R_{1,i}$, $R_{0,i}$ et R [84]. Le but de la définition de facteurs d'importance étendus est donc de comprendre comment calculer ces trois valeurs en fonction du type de macro-événement considéré. Dans la suite, c'est sur le calcul de ces trois valeurs et sur leur signification que nous allons nous focaliser.

1.3 Présentation de l'exemple illustratif

Dans les sections suivantes, différents types d'événements vont être considérés pour le calcul des mesures d'importance. Afin d'aider à la compréhension de leurs différences, et pour pouvoir

les comparer, l'exemple de la figure 3.1 sera utilisé tout au long de ce chapitre. Cet exemple est une simplification de la réalité et n'a qu'une vocation didactique.

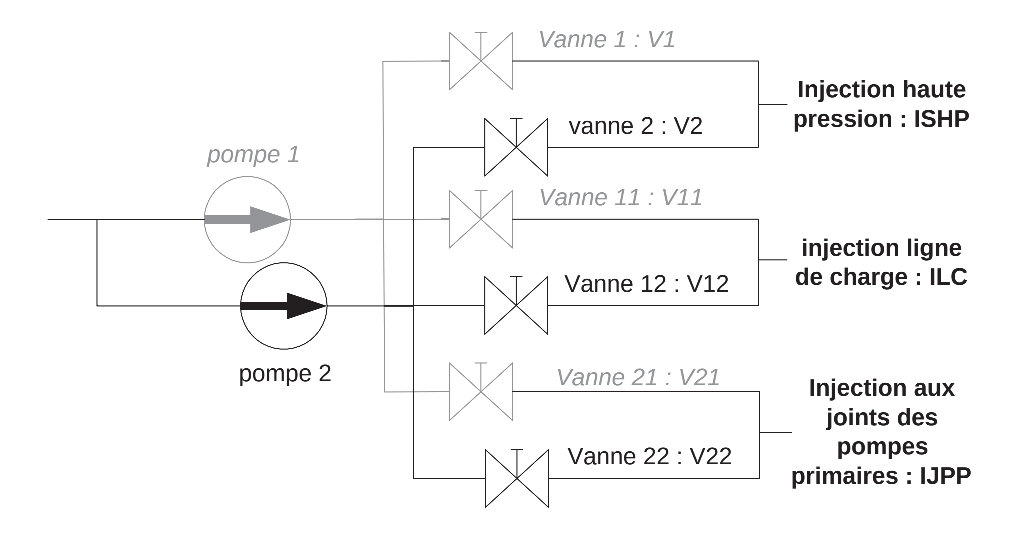


Fig. 3.1 – *Exemple étudié*

On suppose que le modèle EPS se résume au seul arbre d'événements de la figure 3.2 qui modélise les scénarios incidentels ou accidentels possibles suite à l'occurrence de l'initiateur "perte de l'injection aux joints à fuite contrôlée des pompes primaires". Dans la figure 3.2, les séquences associées à la conséquence "CI" sont des séquences qui aboutissent à la fusion du cœur et celles associées à la conséquence "CA" conduisent à des conséquences acceptables. La figure

Perte injection aux joints pompes primaires (IJPP) *Init*	Démarrage refroidissement secours (ASG) *Mission* 1	Injection haute pression 2/2 (ISHP) *Mission* 2	Ligne de charge 1/2 (ILC) *Mission* 3	Injection basse pression (ISBP) *Mission* 4	conseq.
				1	CA
				2	CA
				3	CA
				4	CI
				5	CI

Fig. 3.2 – *Arbre d'événements "perte de l'injection aux joints"*

3.1 présente la partie d'une centrale divisée en deux files. La voie ou file A (en gris) contient les composants avec des numéros impairs. La voie ou file B (en noir) contient les composants avec des numéros pairs. Ces deux files remplissent trois fonctions. La première fonction, notée IJPP, est l'Injection d'eau aux Joints des Pompes Primaires. L'occurrence de sa défaillance correspond à l'occurrence de l'initiateur de l'arbre d'événements de la figure 3.2. Son critère de succès est "une voie au moins fonctionne". La seconde fonction, notée ILC, est l'Injection d'eau via la Ligne de Charge dans le circuit d'eau primaire. Elle correspond à la mission 3 de la figure 3.2. Son critère de succès est "une voie au moins fonctionne". La troisième fonction, notée ISHP, est l'Injection d'eau de Sécurité à Haute Pression dans le circuit primaire. Son critère de succès est "les deux voies sont disponibles". Elle correspond à la mission 2 de la figure 3.2.
Les événements associés à cet exemple sont :

V_{xM} l'événement blocage fermé de la vanne x pour maintenance,
V_{xF} l'événement blocage fermé de la vanne x,

P_{xM} l'événement indisponibilité de la pompe x pour maintenance,
P_{xD} l'événement défaillance en fonctionnement de la pompe x,
E_l le macro-événement correspondant à la perte de l'alimentation électrique des pompes. Cet événement provoque l'arrêt des pompes 1 et 2,
E_{ASG} le macro-événement correspondant à la perte de l'ASG,
E_{ISBP} le macro-événement correspondant à la perte de l'ISBP,
E_{ISHP} le macro-événement correspondant à la perte de l'ISHP,
E_{ILC} le macro-événement correspondant à la perte de l'ILC,
E_{IJPP} le macro-événement correspondant à la perte de l'IJPP.

1.4 Mesure d'importance d'un groupe "Physique, Géographique ou Technologique" (PGT) d'événements de base

1.4.1 Expression des mesures d'importance étendues d'un groupe PGT

Définition des mesures d'importance PGT

Le premier niveau d'application des mesures d'importance étendues que nous avons souhaité redéfinir consiste à considérer l'importance d'un groupe d'événements de base défini à partir de critères physiques et/ou géographiques et/ou techniques. Les événements de base (EB) appartenant à un groupe PGT sont sélectionnés en utilisant séparément ou simultanément trois types de critères :

- des critères géographiques (par exemple, tous les EB modélisant la défaillance de matériels localisés dans la pièce X),
- des critères technologiques (par exemple, tous les EB modélisant la défaillance de vannes pneumatiques),
- des critères physiques (par exemple, tous les EB modélisant la défaillance de matériels reliés par des tuyauteries entre deux points)

Avec des mesures d'importance étendues à des événements PGT, l'événement étudié est l'occurrence ou la non-occurrence simultanée de tous les EB appartenant au groupe PGT. On reprend ainsi la démarche proposée, entre autres, par Cheok dans [20], qui consiste à déterminer l'importance d'un groupe d'événements de base en considérant leur occurrence (respectivement leur non-occurrence) simultanée. Les événements considérés sont alors :

E_{1,PGT_i} l'événement "occurrence de tous les EB du groupe PGT" : $E_{1,PGT_i} = \bigcap_{EB_j \in PGT_i} EB_j$

E_{0,PGT_i} l'événement "non-occurrence de tous les EB du groupe PGT" : $E_{0,PGT_i} = \bigcap_{EB_j \in PGT_i} \overline{EB_j}$

Ainsi, R_{1,PGT_i} est calculé comme le risque sachant que l'événement E_{1,PGT_i} est certain, c'est-à-dire le risque sachant l'occurrence certaine de tous les EB du groupe PGT. De même, R_{0,PGT_i} est calculé comme le risque sachant que l'événement E_{0,PGT_i} est certain, c'est-à-dire le risque sachant que l'occurrence de tous les EB du groupe PGT est impossible.

Calcul des mesures d'importance PGT

R_{1,PGT_i} se calcule comme :

$$R_{1,PGT_i} = P\left(CI/E_{1,PGT_i}\right) = P\left(CI/\bigcap_{EB_j \in PGT_i} EB_j\right)$$

R_{0,PGT_i} se calcule comme :

$$R_{0,PGT_i} = P\left(CI/E_{0,PGT_i}\right) = P\left(CI/\bigcap_{EB_j \in PGT_i} \overline{EB_j}\right)$$

Contrairement à leur définition dans le cadre du risque de référence, R_{1,PGT_i} et R_{0,PGT_i} ne sont pas calculés en considérant l'occurrence et la non-occurrence d'un même événement. En effet, l'événement E_{0,PGT_i} n'est pas la négation logique de l'événement E_{1,PGT_i} (sa négation logique est $\bigcup_{EB_j \in PGT_i} \overline{EB_j}$.).

Expression des FAR et des FDR PGT

Pour illustrer l'extension des mesures d'importance aux groupes PGT, on peut prendre l'exemple du FAR et du FDR. Ainsi, le FAR d'un groupe PGT_i correspond au pourcentage d'augmentation de risque lorsque les événements de base correspondant aux critères d'un groupe PGT sont considérés comme certains.

$$FAR\left(PGT_i\right) = \frac{R_{1,PGT_i} - R}{R} = \frac{P\left(CI/E_{1,PGT_i}\right) - P\left(CI\right)}{P\left(CI\right)} = \frac{P\left(CI/ \bigcap_{EB_j \in PGT_i} EB_j\right)}{P\left(CI\right)} - 1$$

Ainsi, si on crée des critères PGT permettant d'identifier tous les EB correspondant à des défaillances de matériels électriques situés dans un pièce spécifique en-dessous d'une certaine hauteur, le FAR de ce groupe PGT peut correspondre à l'accroissement de risque consécutif à l'inondation de cette pièce.

De même, le FDR d'un groupe PGT_i, exprimé en pourcentage, correspond au pourcentage de diminution de risque lorsque les événements de base correspondant aux critères d'un groupe PGT sont considérés comme impossibles.

$$FDR\left(PGT_i\right) = \frac{R - R_{0,PGT_i}}{R} = \frac{P\left(CI\right) - P\left(CI/E_{0,PGT_i}\right)}{P\left(CI\right)} = 1 - \frac{P\left(CI/ \bigcap_{EB_j \in PGT_i} \overline{EB_j}\right)}{P\left(CI\right)}$$

On a vu dans la section 4.2.1 du chapitre 1 que, lorsque $R_{1,i}$ est calculé à partir des coupes de référence pour un seul EB, certaines coupes ne le contenant pas peuvent devenir non-minimales. De plus, certaines coupes supprimées par le processus de troncation utilisé pour générer les coupes de référence peuvent devenir significatives lorsque l'EB étudié est certain.

Ces deux sources d'incertitude sont encore plus importantes lorsque l'on calcule R_{1,PGT_i} pour un groupe PGT. En effet, si les mesures d'importance sont calculées à partir d'un jeu de coupes correspondant au risque de référence, certaines coupes peuvent devenir non-minimales lorsque l'événement E_{1,PGT_i} est considéré comme certain. De plus, les règles de troncation appliquées pour générer le jeu de coupes correspondant au risque de référence doivent être revues. En effet, certaines coupes très peu probables (et donc souvent supprimées) peuvent voir leur probabilité augmenter fortement et devenir significatives lorsqu'au moins un des EB qui les composent est considéré comme certain, ce qui peut être le cas lorsqu'on calcule R_{1,PGT_i}. Pour résoudre ce problème, on peut recalculer le risque à partir du modèle EPS (et non plus des coupes de référence) en considérant l'événement E_{1,PGT_i} comme certain. Ainsi, Van Der Borst propose dans [84] d'utiliser un modèle EPS rapide ("*fast running PSA*") qui peut être employé pour calculer R_{1,PGT_i} directement à partir du modèle. R_{0,PGT_i}, par contre, peut être calculé avec une très bonne précision à partir des coupes de référence. Une solution alternative peut être d'adapter le processus de troncation des coupes correspondant au risque de référence aux besoins spécifiques des calculs d'importance, comme nous l'avons proposé dans la section 2.1 du chapitre 2.

Exemple de la ligne de charge : Supposons que l'on ait défini un groupe PGT qui correspond aux composants identifiés comme appartenant à la ligne de charge de la figure 1.

Pour permettre cette identification, le groupe PGT associé a pour critère : “tous les composants reliés par des tuyaux entre le début et la fin de la ligne de charge” (pompe 1 et 2, vannes 11 et 12). Les événements de base inclus dans le groupe PGT sont alors ceux qui correspondent à ces quatre composants et qui modélisent leur défaillance ou leur indisponibilité pour maintenance.

On a ainsi :

$$P\left(CI/E_{1,PGT_{ILC}}\right) = P\left(CI/V_{11F} \cap V_{11M} \cap V_{12F} \cap V_{12M} \cap P_{1D} \cap P_{1M} \cap P_{1D} \cap P_{2M}\right)$$

$$P\left(CI/E_{0,PGT_{ILC}}\right) = P\left(CI/\overline{V_{11F}} \cap \overline{V_{11M}} \cap \overline{V_{12F}} \cap \overline{V_{12M}} \cap \overline{P_{1D}} \cap \overline{P_{1M}} \cap \overline{P_{1D}} \cap \overline{P_{2M}}\right)$$

L'événement $E_{0,PGT_{ILC}}$ n'implique pas que la défaillance de l'injection de la ligne de charge ne peut plus se produire. En effet l'événement E_l peut se produire et provoquer l'arrêt des deux pompes.

1.4.2 Application des mesures d'importance PGT

Modéliser l'impact d'une inondation ou d'un incendie

L'association de critères géographiques et technologiques permet, par exemple, de modéliser l'impact d'un incendie ou d'une inondation. Ainsi, le critère géographique “tous les matériels à moins d'un mètre vingt de hauteur” et le critère technologique “tous les matériels électriques” permettent d'estimer le risque $R_{1,PGT_{inond.}}$ qui correspond au risque sachant une inondation interne consécutive à la rupture d'un réservoir (tous les matériels électriques sous l'eau sont défaillants).

Maintenance et tests

Le test d'une voie spécifique ou sa consignation pour maintenance peut impliquer l'indisponibilité de certains matériels. Les modèles développés par EDF incluent des événements de base modélisant l'indisponibilité pour maintenance. Par exemple, on suppose que l'on étudie la maintenance en fonctionnement de la voie A de la ligne de charge. La modélisation de l'indisponibilité de la pompe 1 et de la vanne 11 est présentée dans la figure 3.3. On voit que la

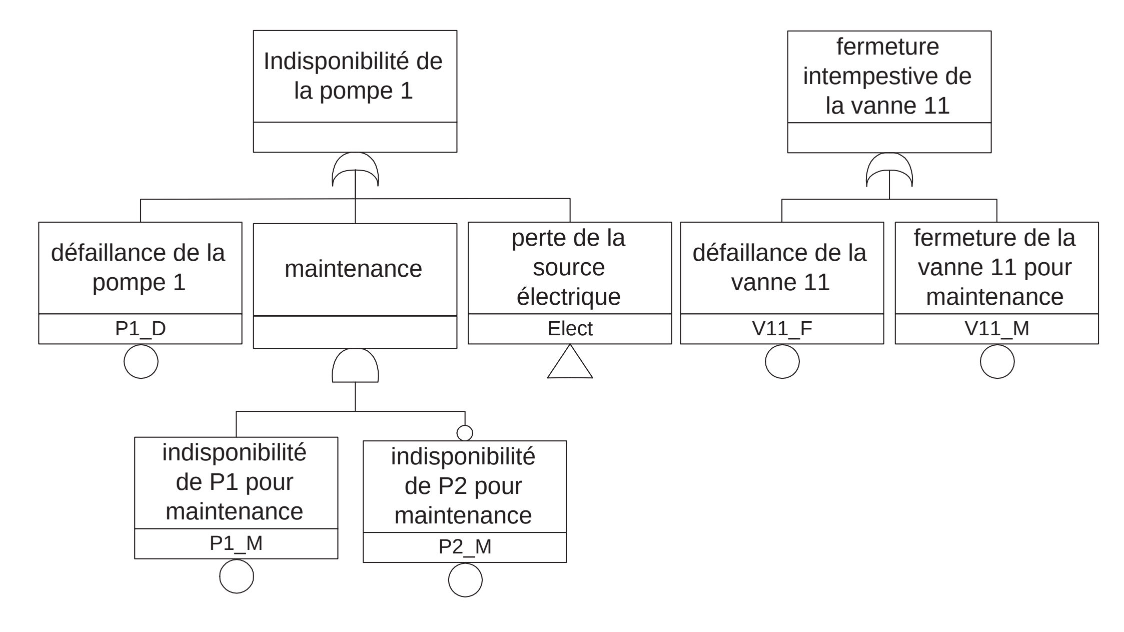


FIG. 3.3 – *Modélisation de la pompe 1 et de la vanne 11*

modélisation des défaillances de ces deux matériels inclut des EB modélisant l'indisponibilité pour maintenance en fonctionnement ($V11_M$ et $P1_M$). Ainsi, le risque sachant que la voie A de la ligne de charge est indisponible pour maintenance peut se calculer en créant un groupe PGT contenant $V11_M$ et $P1_M$. Alors,

$$P\,(CI/indispo.\ voie\ A\ ILC) = P\,(CI/E_{1,PGT_{V\,A}}) = P\,(CI/\,(V11_M \cap P1_M))$$

Le calcul du FAR du groupe $PGT_{Voie\ A}$ ($V11_M$ et $P1_M$ considérés comme certains) permet d'estimer le pourcentage d'accroissement instantané de risque consécutif à la consignation pour maintenance en fonctionnement de la voie A de la ligne de charge. Cet exemple est issu de [42].

Le calcul du FDR du groupe $PGT_{Voie\ A}$ (événements $P1_M$ et $V11_M$ considérés comme impossibles) permet d'estimer la contribution au risque de la maintenance en fonctionnement (sous l'hypothèse que les taux de défaillance de la pompe 1 et de la vanne 11 resteraient inchangés si la maintenance en fonctionnement devenait de la maintenance à l'arrêt).

"Traitement par lot" du calcul des facteurs d'importance au niveau des EB

Dans de nombreuses applications, les différentes mesures d'importance sont estimées pour chaque EB. Pour ce faire, $R_{1,i}$ et $R_{0,i}$ doivent être calculés pour chaque i. Si ces deux valeurs sont obtenues en modifiant et en re-quantifiant le modèle EPS pour chaque EB, le temps de calcul correspondant peut s'avérer très long. Une méthode en deux étapes permet de réduire ce temps de calcul. Tout d'abord, les mesures d'importance sont calculées pour des groupes PGT correspondant à des lots d'événements de base. Ensuite, si certains lots ont une importance qui s'avère négligeable, il n'y a pas lieu de calculer une à une les mesures d'importance des événements de base de ces lots. Ils seront tous négligeables. Habituellement, les critères utilisés pour définir quels EB appartiennent au lot considéré sont des critères physiques reposant sur une vision sommaire des différents systèmes. Les EB appartenant au lot "système i" sont, par exemple, ceux qui correspondent à des matériels situés entre le réservoir X et la vanne Y. Les composants en support des systèmes (composants électriques, distribution d'air comprimé...) ne sont, en général, pas inclus dans ces lots. Des groupes PGT spécifiques sont construits pour les systèmes supports.

Estimation de l'importance d'un système au moyen d'un groupe PGT

Quand on veut connaître l'importance d'un système, une approche au moyen d'un groupe PGT n'est pas pertinente. Même s'il existe des lots définis à partir de visions sommaires des systèmes, il apparaît inapproprié de modéliser la perte d'un système comme la défaillance simultanée de tous ses composants (excepté pour les systèmes parallèles). De plus, si les matériels supports du système étudié (distribution électrique, pneumatique...) ne sont pas inclus dans le groupe PGT, les interdépendances fonctionnelles entre les différents systèmes seront négligées. En revanche, s'ils sont inclus dans le groupe PGT, l'impact sur le risque sera très important car toutes les défaillances possibles de tous les systèmes supports possibles intervenant dans le système étudié seront considérées comme certaines.

Un groupe PGT n'étant pas adapté au calcul de l'importance d'un système, un niveau d'extension des mesures d'importance spécifique doit y être dédié.

1.5 Mesures d'importance d'un système

1.5.1 Expression des mesures d'importance d'un système

Définition d'un système

Principe : Les mesures d'importance étendues peuvent aussi être utilisées pour étudier l'importance d'un système i quand on considère ce système comme une entité remplissant une fonction. Nous définissons donc les composants appartenant à un système comme étant ceux qui contribuent à remplir sa fonction. Dans ce cas, l'événement E_i considéré dans le calcul de $P\,(CI/E_i)$ est l'événement "non-réalisation de la fonction par le système i" (par exemple, la fonction "fournir de l'eau à un débit et une pression donnés" est la fonction définissant la ligne de charge). Cet événement est un événement composé et son occurrence peut être exprimée au

moyen d'une fonction de structure, comme le suggère Dutuit dans [36]. La négation logique au moyen des règles de Morgan est utilisée pour définir l'événement $\overline{E_i}$. Avec un modèle booléen, l'événement E_i peut être exprimé comme l'union des coupes minimales modélisant la perte de la fonction qui définit le système i ($CM_{Syst.}$). L'événement $\overline{E_i}$ correspond à la non-occurrence de ces $CM_{Syst.}$ ou, de manière équivalente, à l'occurrence d'au moins un chemin de succès du système i.

Signification : Quand l'événement "défaillance du système i" est considéré comme certain, la seule information disponible est que la fonction n'est plus remplie, c'est-à-dire qu'une des coupes du système CM_{Syst} est réalisée. On ne connaît pas de manière certaine quel est ou quels sont les matériels défaillants. $P\left(CI/E_{Syst.\,i}\right)$ correspond alors au risque sachant que la défaillance du système i est observée (événement$E_{Syst.\,i}$) mais que la cause de cette défaillance n'est pas diagnostiquée. Si la cause ou les causes de la défaillance du système sont connues, c'est-à-dire si la coupe réalisée est connue, un groupe PGT incluant les composants défaillants modélisera plus précisément le risque sachant la/les défaillances.

En exprimant $P\left(CI/E_{Syst.\,i}\right)$ au moyen d'un développement de Poincaré à l'ordre 1 (simplification acceptable si l'hypothèse des événements rares est validée), on trouve que :

$$P\left(CI/E_{Syst.\,i}\right) = \frac{P\left(CI \cap E_{Syst.\,i}\right)}{P\left(E_{Syst.\,i}\right)} = \frac{P\left(\bigcup_{CM_{Syst.\,i} \in E_{Syst\,i}} CI \cap CM_{Syst\,i}\right)}{P\left(E_{Syst.\,i}\right)}$$

$$\underset{\substack{hypoth\grave{e}se\ des \\ \acute{e}v\acute{e}nements\ rares}}{\approx} \sum_{CM_{Syst.\,i} \in E_{Syst\,i}} P\left(CI/CM_{Syst\,i}\right) \cdot \frac{P\left(CM_{Syst.\,i}\right)}{P\left(E_{Syst.\,i}\right)}$$

avec $CM_{Syst.\,i}$ une des coupes minimales de l'événement $E_{Syst.\,i}$.

En première approximation, on peut donc exprimer $R_{1,i}$ pour un système comme la somme des probabilités conditionnelles de CI sachant une coupe de ce système pondérée par la contribution de cette coupe à la probabilité de perte du système.

Calcul des mesures d'importance de systèmes

Comme on l'a vu dans la section 1.2, la connaissance de $R_{1,Syst.}$ (le risque sachant que le système i est défaillant) et de $R_{0,Syst.}$ (le risque sachant que le système i n'est pas défaillant) suffit à calculer l'ensemble des mesures d'importance étendues. Le calcul de ces deux valeurs n'est pas prévu dans tous les logiciels supports des EPS. Toutefois, ces deux risques peuvent être exprimés comme :

$$\begin{aligned} R_{1,Syst.} &= P\left(CI/E_{Syst\,i}\right) &&= \frac{P\left(CI \cap E_{Syst\,i}\right)}{P\left(E_{Syst\,i}\right)} \\ R_{0,Syst.} &= P\left(CI/E_{Syst\,i}\right) &&= \frac{P\left(CI \cap \overline{E_{Syst\,i}}\right)}{P\left(\overline{E_{Syst\,i}}\right)} \\ & &&= \frac{P\left(CI\right) - P\left(CI \cap E_{Syst\,i}\right)}{1 - P\left(E_{Syst\,i}\right)} \end{aligned}$$

avec :

$E_{Syst\,i}$ l'événement "occurrence de la défaillance du système i" : $E_{Syst\,i} = \bigcup CM_{Syst\,i}$

$\overline{E_{Syst\,i}}$ l'événement "non-occurrence de la défaillance du système i" : $\overline{E_{Syst\,i}} = \bigcap \overline{CM_{Syst\,i}}$

On voit alors que la connaissance de $P\left(E_{Syst.}\right)$, de $P\left(CI \cap E_{Syst\,i}\right)$ et de $P\left(CI\right)$ suffit à calculer les mesures d'importance étendues au niveau des systèmes.

L'ensemble de ces valeurs peut être calculé à partir de RSW. Ainsi, pour déterminer $P\left(E_{Syst.}\right)$ et $P\left(CI \cap E_{Syst\,i}\right)$, l'arbre de défaillances modélisant la perte du système i doit être construit. Quand on quantifie cet arbre seul, on détermine $P\left(E_{Syst.}\right)$. Pour déterminer

$P\left(CI \cap E_{Syst\ i}\right)$, on peut utiliser l'arbre d'événements de la figure 3.4. Cet arbre d'événements commence par un initiateur de type "conséquence" qui correspond à l'événement CI. Cet initiateur regroupe sous une porte OU toutes les coupes correspondant à l'événement CI. La séquence 2 de cet arbre d'événements correspond à $P\left(CI \cap E_{Syst\ i}\right)$.

Initiateur de type conséquence associé à CI	Perte du système i		conseq.
		1	CI et pas $Syst_i$
		2	CI et $Syst_i$

FIG. 3.4 – *Arbre d'événements fictif servant au calcul des mesures d'importance de systèmes*

Si le modèle utilisé ne repose pas sur l'utilisation d'arbres d'événements, la probabilité $P\left(CI \cap E_{Syst\ i}\right)$ peut être calculée de manière équivalente en regroupant sous une porte ET la porte sommet correspondant à l'événement non souhaité (CI) et la porte sommet de l'arbre de défaillances modélisant la défaillance du système i, comme le montre la figure 3.5.

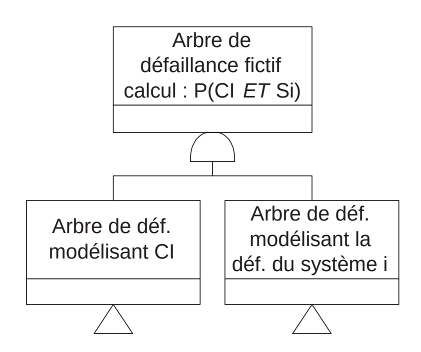


FIG. 3.5 – *Arbre de défaillances fictif servant au calcul de* $P\left(CI \cap E_{Syst\ i}\right)$

Exemple de l'importance du système ligne de charge : Supposons que les capteurs mesurant le débit de la ligne de charge indiquent que celui-ci est nul mais qu'on ne sache pas la cause de la perte de ce système. Le FAR du système "ligne de charge" peut être calculé pour déterminer l'accroissement de risque résultant de cette perte. Supposons que l'événement "perte de la ligne de charge" puisse être exprimé comme :

$$(P_1 \cap P_2) \cup (P_1 \cap V_{12}) \cup (V_{11} \cap P_2) \cup (V_{11} \cap V_{12}) \cup E_l$$

Avec les simplifications suivantes : $P_i = P_{iM} \cup P_{iF}$ et $V_i = V_{iM} \cup V_{iF}$. E_l est un macro-événement modélisant la perte des alimentations électriques. On a alors :

$$\begin{aligned}
& P\left(CI/E_{ILC}\right) \\
& = P\left(CI/\left(P_1 \cap P_2\right) \cup \left(P_1 \cap V_{12}\right) \cup \left(V_{11} \cap P_2\right) \cup \left(V_{11} \cap V_{12}\right) \cup E_l\right) \\
& = \frac{P\left(CI \cap E_{ILC}\right)}{P\left(E_{ILC}\right)} \\
& \underset{\substack{\text{hypothèse} \\ \text{événements rares}}}{\approx} \underbrace{\frac{P\left(CI \cap P_1 \cap P_2\right)}{P\left(E_{ILC}\right)}}_{\text{ISHP, ILC et IJPP sont def}} + \underbrace{\frac{P\left(CI \cap E_l\right)}{P\left(E_{ILC}\right)}}_{\substack{\text{Tous les matériels électriques} \\ \text{sont défaillants}}} \\
& + \underbrace{\frac{P\left(CI \cap P_1 \cap V_{12}\right)}{P\left(E_{ILC}\right)} + \frac{P\left(CI \cap V_{11} \cap P_2\right)}{P\left(E_{ILC}\right)}}_{\text{ISHP et ILC défaillants, perte de redondance pour IJPP}} \\
& + \underbrace{\frac{P\left(CI \cap V_{11} \cap V_{12}\right)}{P\left(E_{ILC}\right)}}_{\substack{\text{ILC défaillant. Les autres ne} \\ \text{sont pas défiabilisés}}}
\end{aligned}$$

Comme on le voit ci-dessus, toutes les configurations correspondant à la perte de la ligne de charge sont considérées.

1.5.2 Application des mesures d'importance de systèmes

Le FAR d'un système représente l'augmentation instantanée du risque lorsqu'une fonction est perdue. Ce type d'information pourrait s'avérer utile pour optimiser la conduite à tenir face à la perte d'un système (indisponibilité non diagnostiquée d'un système) ou pour aider à la gestion du risque lors d'indisponibilités provoquées.

1.6 Mesure d'importance d'une fonction

1.6.1 Expression des mesures d'importance étendues au niveau d'une fonction

Définition de l'importance d'une fonction

Les mesures d'importance étendues peuvent être utilisées pour étudier l'importance d'une fonction indépendamment des matériels qui la supportent. La question à laquelle nous souhaitons répondre est alors "Quel serait le risque si la fonction étudiée n'existait pas ?" et non pas "Quel serait le risque si la fonction étudiée n'était plus remplie suite à la défaillance du système qui la supporte ?" (comme dans le cas des mesures d'importance d'un système). Une formulation équivalente pourrait être "Quel serait le risque si la fonction étudiée n'était plus remplie du fait d'une défaillance intrinsèque ?" avec la défaillance intrinsèque d'une fonction définie comme une défaillance d'un ou de plusieurs composants qui implique la perte de la fonction et qui n'affecte aucunement les autres systèmes. Une autre question intéressante est "Quel est le risque lorsque la fonction étudiée est toujours remplie ?" et non pas "Quel est le risque lorsque les composants supportant la fonction ne peuvent pas défaillir ?".

Lorsque les mesures d'importance d'une fonction sont calculées, tous les composants (même ceux supportant la fonction) garde leur probabilité de défaillance de référence, c'est-à-dire leur probabilité de défaillance lorsqu'on calcule le risque de référence. Tous les événements de base gardent leur probabilité d'occurrence de référence.

Calcul des mesures d'importance d'une fonction

Comme on l'a vu précédemment, le fait que l'on considère une fonction comme étant défaillante ou toujours remplie n'affecte la fiabilité d'aucun composant. La non-existence d'une fonction ou son parfait fonctionnement sont modélisés en changeant la structure du modèle (et non pas l'état des différents composants).

Pour prendre en compte, au moyen d'un modèle incluant des arbres d'événements, le fait qu'une fonction est toujours remplie, on cherche l'événement en tête qui correspond à la perte de la fonction étudiée. On considère alors cet événement comme impossible (l'événement est mis à "FAUX" dans le modèle). On ne considère alors que la branche de succès de l'arbre d'événements. Si le modèle utilisé ne contient que des arbres de défaillance, il faut rechercher la porte logique correspondant à l'échec de la fonction et la déclarer comme étant non-réalisée (la porte est mise à "FAUX").

Pour prendre en compte, au moyen d'un modèle incluant des arbres d'événements, le fait qu'une fonction est toujours défaillante ou n'existe plus, on cherche l'événement en tête dans le ou les arbres d'événements qui correspond à la fonction étudiée. On déclare alors cet événement comme étant toujours réalisé (l'événement est mis à "VRAI" dans le modèle). Si le modèle utilisé ne contient que des arbres de défaillance, il faut rechercher la porte logique correspondant à l'échec de la fonction et la déclarer comme étant réalisée (la porte est mise à "VRAI").

Exemple : Supposons qu'on s'intéresse à la fonction "injection par la ligne de charge" et supposons que l'arbre d'événements de la figure 3.2 est le modèle EPS entier. Alors $P\left(CI/E_{ILC}\right)$ est calculé au moyen du modèle de la figure 3.6. On notera que dans ce modèle, la séquence 2 n'est plus possible.

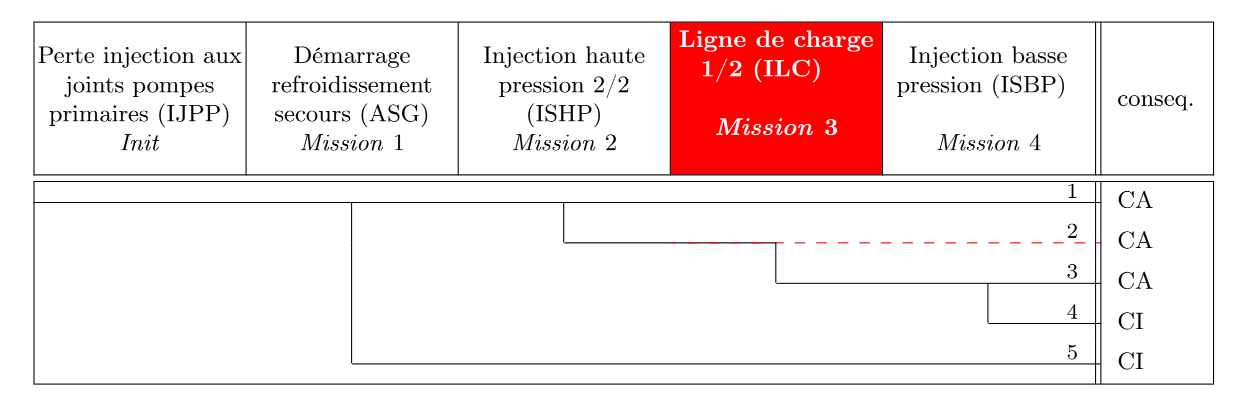


FIG. 3.6 – *Arbre d'événements modifié pour calculer* $P\left(CI/E_{ILC}\right)$

$P\left(CI/\overline{E_{ILC}}\right)$ est calculé de la même façon au moyen de l'arbre d'événements de la figure 3.7. Dans cet arbre, les séquences 3 et 4 ne sont plus possibles car elles contiennent la défaillance de la ligne de charge.

Perte injection aux joints pompes primaires (IJPP) *Init*
Démarrage refroidissement secours (ASG) *Mission* 1
Injection haute pression 2/2 (ISHP) *Mission* 2
Ligne de charge 1/2 (ILC) *Mission* 3
Injection basse pression (ISBP) *Mission* 4
conseq.
1 CA
2 CA
3 CA
4 CI
5 CI

FIG. 3.7 – *Arbre d'événements modifié pour calculer* $P\left(CI/\overline{E_{ILC}}\right)$

Si on suppose maintenant que notre modèle ne contient pas d'arbres d'événements, l'arbre de défaillances correspondant à l'événement CI est donc celui de la figure 3.8. Cet arbre de défaillances est équivalent à l'arbre d'événements de la figure 3.2.

$P\left(CI/E_{ILC}\right)$ est calculé en mettant à "VRAI" la porte ILC de la figure 3.8, qui correspond à l'événement "défaillance de la ligne de charge". L'arbre de défaillances équivalent est celui de la figure 3.9. $P\left(CI/\overline{E_{ILC}}\right)$ est calculé en mettant à "FAUX" la porte ILC de la figure 3.8, qui correspond à l'événement "défaillance de la ligne de charge". L'arbre de défaillances équivalent est celui de la figure 3.10. De la même façon, si on veut calculer l'importance des missions ISHP, ISBP ou ASG, on mettra les portes correspondantes à VRAI ou à FAUX. Ainsi, le risque sachant que la mission Injection de Secours Haute Pression n'existe plus se calculera avec l'arbre de la figure 3.11.

1.6.2 Applications des mesures d'importance calculées au niveau des fonctions

Dans cette section, seules des applications potentielles des mesures d'importance calculées au niveau des fonctions sont présentées.

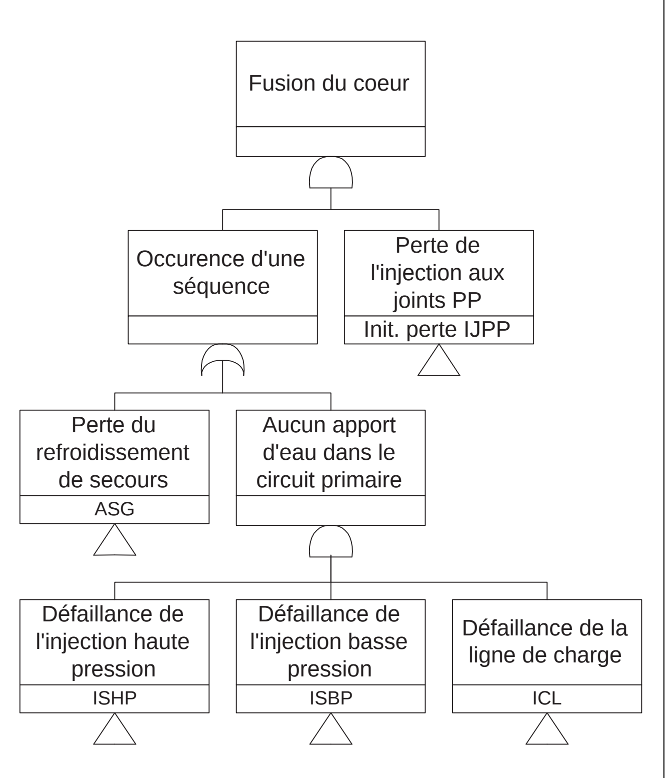


FIG. 3.8 – *Arbre de défaillances modélisant l'événement CI*

Fusion du coeur
Occurence d'une séquence
Perte de l'injection aux joints PP
Init. perte IJPP
Perte du refroidissement de secours
ASG
Aucun apport d'eau dans le circuit primaire
Défaillance de l'injection haute pression
ISHP
Défaillance de l'injection basse pression
ISBP

FIG. 3.9 – *Arbre de défaillances pour le calcul de* $P\left(CI/E_{ILC}\right)$

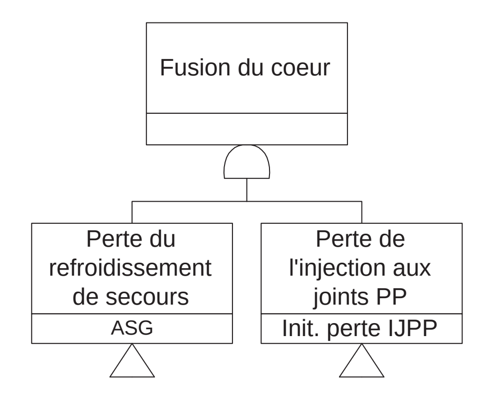


FIG. 3.10 – *Arbre de défaillances pour le calcul de* $P\left(CI/\overline{E_{ILC}}\right)$

Aide à la conception

Lors de la conception d'une nouvelle centrale, un modèle EPS peut être développé pour estimer le risque a priori. Ce modèle peut être utilisé pour tester de nouveaux systèmes, tester de nouvelles fonctions, etc. Dans ce cadre, il peut être intéressant de connaître l'importance de chaque fonction, comme le suggère le rapport NUREG-4377 [95].

Modification des centrales existantes

Durant la vie d'une centrale, des modifications fonctionnelles et organisationnelles sont apportées pour intégrer l'expérience acquise depuis sa conception. Leur but peut être de diminuer

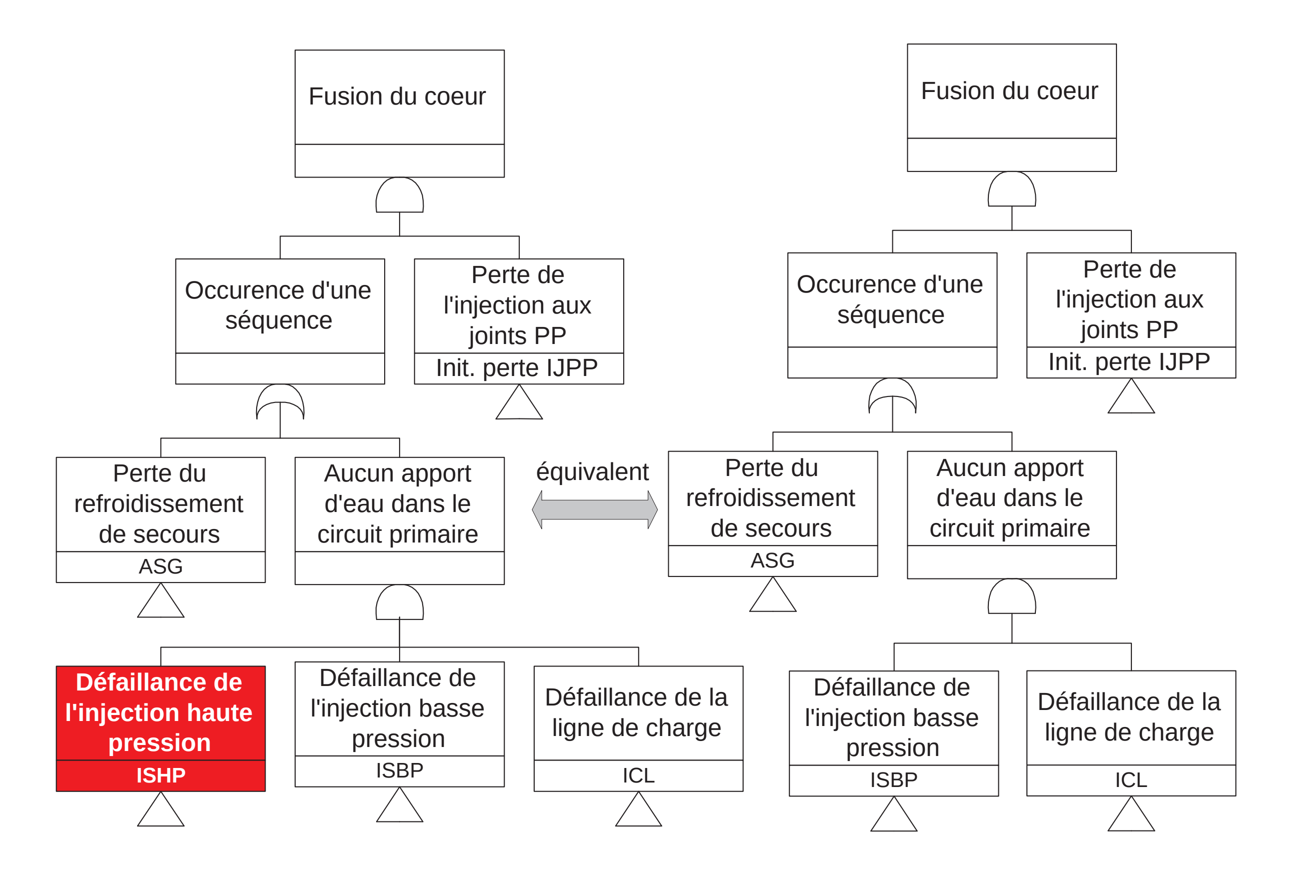


FIG. 3.11 – *Arbre de défaillances pour le calcul de* $P\left(CI/E_{ISHP}\right)$

le niveau de risque ou d'augmenter, à risque constant, la disponibilité de la centrale. Avant de procéder à des modifications fonctionnelles, on les teste au moyen de modèles EPS. L'apport de la ou des nouvelles fonctions envisagées peut être mesuré au moyen de mesures d'importance de fonction.

Interdépendances entre fonctions

La comparaison du FAR d'une fonction et de celui du système remplissant cette fonction fournit une évaluation de la dépendance entre ce système et le reste de la centrale. En effet, si le système étudié est totalement indépendant des autres systèmes de la centrale, alors $FAR_{Système\ i}\left(E_i\right) - FAR_{Fonction\ i}\left(E_i\right) = 0$. En revanche, s'il y a une forte dépendance entre le système i et d'autres systèmes de la centrale (par exemple du fait de matériels partagés entre plusieurs systèmes), $FAR_{Système\ i}\left(E_i\right) \gg FAR_{Fonction\ i}\left(E_i\right)$.

Quand on conçoit les systèmes d'un nouveau type de centrale, il peut être intéressant de tester par ce biais leur indépendance, de manière à limiter le nombre et l'importance des modes communs fonctionnels. Ce type de problématique sera repris et développé dans le chapitre 4.

1.7 Application numérique comparative

L'objectif de cette application numérique est de comparer l'importance de différents macro-événements qui correspondent aux différents niveaux auxquels nous proposons d'étendre les mesures d'importance. Elle permet aussi d'illustrer les applications qui peuvent être faites de ces mesures d'importances étendues.

Pour réaliser cette application numérique, on considère que le modèle EPS se résume à l'arbre d'événements de la figure 3.2. La modélisation de la ligne de charge (ILC), de l'injection

de sécurité haute pression (ISHP), de l'alimentation de secours des générateurs de vapeur (ASG) et de l'injection de sécurité basse pression (ISBP) sont présentées dans l'annexe A.

On s'intéresse aux mesures d'importance étendues à différents niveaux pour la ligne de charge (ILC) et pour l'injection de sécurité basse pression (ISBP). Les quatre niveaux considérés sont :

– l'importance du groupe PGT correspondant à la maintenance de la voie A (uniquement pour la ligne de charge),
– l'importance du groupe PGT correspondant à la définition sommaire du système dans l'approche par lots,
– l'importance du système (approche fonctionnelle rigoureuse),
– l'importance de la fonction du système (indépendamment du système).

Définition des événements considérés

Les événements considérés sont les suivants :
- Le groupe PGT correspondant à la maintenance de la voie A de la ligne de charge contient l'EB P_{1M} ;
- le groupe PGT correspondant à la ligne de charge inclut les événements P_{1D}, P_{2D}, V_{11F} et V_{12F}. Il est obtenu au moyen du critère physique : "les matériels situés entre l'arrivée d'eau et la sortie de la ligne de charge". Il n'inclut en particulier pas bon nombre de systèmes supports (dans notre cas, l'alimentation électrique) ;
- le système "ligne de charge" est défini à partir de la fonction "fournir de l'eau à un débit donné et à une pression donnée dans au moins une voie sur deux". L'arbre de défaillances qui modélise la perte de ce système est présenté en annexe dans la figure A.3 de l'annexe A ;
- la mission qu'on appellera ILC est la mission 3 de l'arbre d'événements de la figure 3.2 (l'événement en tête "ligne de charge 1/2") ;
- le groupe PGT correspondant à l'injection de sécurité basse pression contient l'EB `ISBP_int_D`. Il est obtenu au moyen du critère physique : "les matériels situés entre l'arrivée d'eau et la sortie de l'injection de sécurité basse pression". Il n'inclut en particulier pas ses systèmes supports (dans notre cas, l'alimentation électrique) ;
- le système "injection de sécurité basse pression" est défini à partir de la fonction "fournir de l'eau à un débit et à une pression donnés". L'arbre de défaillances modélisant la perte de ce système est présenté en annexe dans la figure A.6 de l'annexe A ;
- la mission qu'on appellera ISBP est la mission 4 de l'arbre d'événements de la figure 3.2 (l'événement en tête "injection basse pression").

Résultats numériques

Les données pour la ligne de charge et l'injection basse pression sont :

	événement	FAR	FDR
ILC	maintenance voie A	$FAR\,(E_{1,PGT\ voie\ A}) \approx 249$	$FDR\,(E_{1,PGT\ voie\ A}) \approx 25\%$
	PGT ILC	$FAR\,(E_{1,PGT\ ILC}) \approx 167000$	$FDR\,(E_{1,PGT\ ILC}) \approx 83\%$
	système ILC	$FAR\,(E_{Syst;ILC}) \approx 73000$	$FDR\,(E_{Syst;ILC}) \approx 58\%$
	fonction ILC	$FAR\,(E_{fonct;ILC}) \approx 0{,}33$	$FDR\,(E_{fonct;ILC}) \approx 33\%$
ISBP	PGT ISBP	$FAR\,(E_{1,PGT\ ISBP}) \approx 2503$	$FDR\,(E_{1,PGT\ ISBP}) \approx 33\%$
	système ISBP	$FAR\,(E_{Syst;ISBP}) \approx 3365$	$FDR\,(E_{Syst;ISBP}) \approx 33\%$
	fonction ISBP	$FAR\,(E_{fonct;ISBP}) \approx 2503$	$FDR\,(E_{fonct;ISBP}) \approx 33\%$

TAB. 3.1 – *FAR et FDR des différents macro-événements de l'application numérique*

Interprétation de ces résultats

De ces différents résultats, on peut tirer les informations suivantes :

Maintenance : La maintenance de la voie A de la ligne de charge a un impact important sur le risque. Si cette maintenance en ligne devenait de la maintenance à l'arrêt (et sous réserve que sa fiabilité n'en soit pas affectée), le risque diminuerait de 25% (valeur de $FDR\,(E_{1,PGT\ voie\ A})$). De plus, l'augmentation instantanée du risque consécutive à l'arrêt pour maintenance de la voie A ($FAR\,(E_{1,PGT\ voie\ A})$) est très importante. Cette maintenance en ligne doit donc être remise en cause et, si on ne peut pas la supprimer, sa durée doit être réduite autant que possible.

Importance des systèmes : Bien qu'on puisse noter que le FAR du groupe PGT ILC ($FAR\,(E_{1,PGT\ ILC})$) est plus grand que celui du système ILC ($FAR\,(E_{Syst;ILC})$) et bien qu'une approche PGT des FAR implique que tous les composants considérés de manière sommaire comme appartenant au système soient défaillants, on ne peut pas conclure que le FAR_{PGT} d'un système est un majorant du $FAR_{Syst.}$ de ce même système. Cette affirmation est fausse en général. En effet, le FAR d'un système inclut des événements (défaillance des matériels supports par exemple) qui ne sont pas considérés dans le groupe PGT correspondant à une approche physique (et non fonctionnelle) de ce système. Le cas de l'ISBP l'illustre. En effet, le FAR du système ISBP ($FAR\,(E_{Syst;ISBP})$) est très supérieur à celui du groupe PGT ISBP ($FAR\,(E_{1,PGT\ ISBP})$) car lorsque la défaillance du système ISBP est considérée, on envisage le cas où une défaillance électrique (qui affecte tous les autres systèmes) cause la perte de l'injection basse pression alors que ce type de défaillance n'est, en général, pas considéré dans les groupes PGT.

Interdépendances entre systèmes : Certains systèmes partagent des composants. Lorsque l'un de ces systèmes est défaillant, cela peut être dû à certains des composants qui lui sont propres mais aussi à des composants partagés par d'autres systèmes. Ainsi, lorsque l'un de ces systèmes est défaillant sans qu'on en sache la cause, c'est potentiellement un sous-système partagé qui est défaillant et une défaillance des autres systèmes est alors plus vraisemblable. C'est le cas pour la ligne de charge. Quand la défaillance du système ligne de charge est considérée comme certaine, le FAR calculé est énorme (73000) alors que l'importance de la fonction ligne de charge est beaucoup plus faible : son FAR est de 0,33. En effet, lorsque l'on considère la défaillance certaine du système ligne de charge (pour calculer le FAR du système ligne de charge), on se rend compte que ce système est le plus souvent perdu suite à la défaillance des deux pompes. De plus, lorsque ces pompes sont défaillantes, la défaillance de l'injection aux joints et de l'injection haute pression sont certaines et le risque est donc très important. Lorsqu'on calcule le risque sachant la perte de la ligne de charge, on considère donc principalement le risque sachant la défaillance des pompes, qui est très élevé. C'est à dire qu'on considérera non seulement l'impact de la perte de la fonction ILC, qui est égal à $R_{1,fonct;ILC}$, mais en plus on considérera l'impact de la défaillance des matériels de la ligne de charge sur les autres systèmes. Si les autres systèmes ne partageaient aucun matériel avec la ligne de charge, ce second impact serait nul, mais ce n'est pas le cas dans notre exemple.

Quand le FAR du système ligne de charge est comparé au FAR de la fonction ligne de charge, l'écart s'explique par les implications potentielles sur les autres systèmes de la perte de la ligne de charge.

Les résultats de notre exemple fictif montrent que ni la ligne de charge ni l'injection basse pression ne sont des systèmes parfaitement indépendants des autres systèmes de sauvegarde de la centrale. En effet, le FAR du système ISBP est supérieur à celui de la fonction ISBP ($FAR\,(E_{Syst;ISBP}) > FAR\,(E_{fonct;ISBP})$) de même pour l'injection de la ligne de charge

$(FAR(E_{Syst;ILC}) \gg FAR(E_{fonct;ILC}))$; ces écarts traduisent dans le cas du système ILC le fait qu'il partage la pompe 1 et la pompe 2 avec les systèmes IJPP et ISHP et que ce système ILC partage son alimentation électrique avec tous les autres systèmes. Dans le cas de l'ISHP, l'écart entre FAR de système et FAR de fonction est plus faible car le seul lien avec les autres systèmes est son alimentation électrique, qui est relativement fiable.

Le FAR de la fonction ligne de charge est relativement faible (0,33). Cette fonction pourrait donc être considérée comme relativement peu importante mais le FDR de cette fonction est significatif. Le risque décroîtrait donc de manière importante si cette fonction était toujours remplie. De plus, le FAR du système ILC est très élevé comparé au FAR de la fonction. Ces trois informations doivent conduire à la conclusion qu'il y a trop de dépendances fonctionnelles entre le système "ligne de charge" et les systèmes dont il doit amoindrir les conséquences des défaillances. Ces interdépendances fonctionnelles doivent être réduites pour améliorer l'apport de la ligne de charge en termes de diminution de risque.

2 La gestion des cumuls d'indisponibilité

Pour permettre une bonne gestion des risques lors de l'exploitation des centrales nucléaires d'EDF, des "règles d'exploitation" ont été élaborées. Parmi ces règles, les Spécifications Techniques d'Exploitation (STE) permettent entre autres de savoir quels sont les matériels ou les sous-systèmes dont l'occurrence de la défaillance nécessite une conduite de la centrale particulière. Pour les matériels ou les sous-systèmes les plus importants, qui sont dits "*de groupe 1*", les STE définissent une "*délai d'amorçage de repli*" qui correspond au temps dont l'exploitant dispose pour réparer les matériels défaillants avant d'avoir à "replier" la centrale (arrêt de la réaction de fission et atteinte d'un état, en termes de température et de pression du circuit primaire, dans lequel le matériel indisponible n'est plus important pour le risque). Lorsqu'un matériel ou un sous-système dit "*de groupe 1*" est indisponible, on parle d'un "*événement de groupe 1*".

Notre objectif est de voir comment une démarche utilisant les facteurs d'importance peut aider à l'optimisation des délais avant repli lorsque deux événements de groupe 1 se produisent simultanément.

2.1 Contexte industriel : les Spécifications Techniques d'Exploitation (STE)

Un événement de groupe 1 peut être provoqué alors que la centrale est en production si les STE l'autorisent. Il peut être nécessaire à la réalisation d'une action de maintenance. On parle alors de "*condition limite*" pour "*l'événement de groupe 1*" considéré. Toutefois, l'emploi d'une condition limite est très réglementé. Ainsi, dans [38] (chapitre DEF), on peut lire : "*Une condition limite est une condition qui autorise le fonctionnement de la tranche non en conformité stricte avec une prescription. Cette condition limite ne doit être utilisée que le temps nécessaire à la réalisation des impératifs d'exploitation (conduite / maintenance / contrôle). Aux conditions limites peuvent être associées des précautions particulières ou des mesures palliatives qui doivent être respectées.*"

Les délais de repli associés à un événement de groupe 1 (condition limite ou événement fortuit) sont issus de deux sources. Ils sont pour la plupart définis par avis d'expert mais quelques-uns ont été déterminés à partir des EPS. Dans ce cas, le délai de repli T_i d'un événement i de groupe 1 est calculé de telle sorte que l'accroissement de risque consécutif à la condition limite ne soit pas supérieur à 10^{-7}.

Toutefois, lorsqu'une condition limite est en cours, un événement fortuit de groupe 1 peut se produire. Dans ce cas, une règle de cumul est appliquée pour définir le nouveau délai avant

repli. La règle permettant de définir le délai de repli est la suivante : "*Le délai alloué à un cumul de deux indisponibilités associées respectivement aux délais T_1 et T_2 est égal à la valeur de référence immédiatement inférieure au plus petit des deux délais* [les valeurs de références pour un délai de repli sont 1h, 8h, 1j, 3j et 7j]. *Dans le cas où le plus petit délai est égal à 1 heure, le délai du cumul sera pris aussi égal à 1 heure*". La règle des cumuls d'indisponibilité définie par les STE peut donc être résumée par le tableau 3.2.

		T_1				
		1h	8h	1j	3j	7j
T_2	1h	1h	1h	1h	1h	1h
	8h	1h	1h	1h	1h	1h
	1j	1h	1h	8h	8h	8h
	3j	1h	1h	8h	1j	1j
	7j	1h	1h	8h	1j	3j

TAB. 3.2 – *Tableau récapitulatif des délais de repli en cas de cumul d'un condition limite et d'un événement de groupe 1 fortuit*

Avantage de la règle de gestion des cumuls existante

Cette règle a le très grand mérite d'être simple. Quelle que soit la condition limite considérée, quel que soit l'événement de groupe 1 fortuit considéré, elle est appliquée de la même façon. De plus, les très courts délais de repli peuvent laisser penser que cette règle de gestion des cumuls est conservative, c'est-à-dire qu'on peut raisonnablement penser que les délais définis pour les cumuls correspondent à des accroissements de risque inférieurs à 10^{-7}.

Inconvénient de cette règle

Puisque cette règle de cumul n'est pas basée sur les EPS, rien ne garantit que les délais prescrits avant repli ne soient pas trop optimistes dans certains cas. Cela revient à dire qu'on ne peut pas garantir que, pour une condition limite CL_1 et un événement fortuit E_2 de groupe 1, l'accroissement de risque associé à la configuration CL_1 et E_2 durant une durée $T_{CL_1;E_2}$ (obtenue en appliquant la règle des cumuls) ne soit pas supérieur à 10^{-7}.

A l'inverse, puisque cette règle n'est pas basée sur une étude des accroissements de risques, on peut supposer que, dans de nombreux cas, elle est beaucoup trop restrictive. C'est à dire qu'on peut supposer que l'accroissement de risque consécutif à la configuration CL_1 et E_2 durant une durée $T_{CL_1;E_2}$ est bien inférieur à 10^{-7} pour de nombreux cumuls.

Par exemple, supposons que la pompe 1 de la voie A de la ligne de charge du système présenté dans le schéma de la figure 3.1 soit indisponible pour maintenance. Supposons aussi que la perte de la voie A de l'injection de sécurité haute pression (ISHP) soit un événement de groupe 1. Dans ce cas, lorsque la voie A de la ligne de charge fait l'objet d'une condition limite et que l'événement "perte de la voie A de l'ISHP" survient (par exemple, à cause du blocage fermé de la vanne V_1 suite à un test), on aura un délai de repli très court. Pourtant, l'occurrence de la défaillance de la voie A de l'ISHP sachant que la pompe 1 fait l'objet d'une condition limite n'a aucun impact sur le risque. En effet, la défaillance de la vanne 1 alors qu'elle ne peut plus être alimentée par la pompe 1, arrêtée pour maintenance, n'a aucun impact. Dans ce cas, le délai avant repli devrait être la plus petite valeur entre T_{P_1} (pour la pompe 1) et T_{V_1} (pour la vanne 1).

Supposons que que $T_{P_1} = 8$h et que $T_{V_1} = 1$ jour. Supposons T_{P_1} et T_{V_1} ont été définis à partir des EPS de telle sorte que l'accroissement de risque consécutif à la panne de la pompe durant 8 heures ou celui consécutif à un blocage fermé de la vanne durant une journée soit égal à 10^{-7}. La règle de cumul actuelle imposera d'arrêter la production au bout d'une heure

(c.f. 3.2) si la vanne ou la pompe ne sont pas remises en marche durant ce délai. Pourtant, on dispose de 8 heures avant que l'accroissement de risque consécutif à la panne de la pompe et au blocage de la vanne ne dépasse 10^{-7}. Dans le cas de cet exemple, la règle actuelle de gestion des cumul est donc très conservative.

2.2 Quels indicateurs pour la gestion des cumuls

Dans cette section, nous présentons la démarche d'élaboration des indicateurs de risque potentiellement utilisables pour la gestion des cumuls d'événements de groupe 1.

2.2.1 Calcul du risque en cas de cumul

Avant de proposer une démarche pour identifier les cumuls d'événements augmentant le risque ou ceux affaiblissant le niveau de défense en profondeur, il faut au préalable définir comment on estime le risque en cas de cumul.

Dans la suite de ce chapitre, nous utilisons les notations suivantes. L'événement "existence d'une condition limite j" est noté CL_j. L'événement fortuit i qui est de groupe 1 est noté E_i.

Ces deux événements peuvent n'être considérés que sur un état de la centrale. Pour mémoire, les états considérés dans les EPS sont :
- État A : tranche en puissance,
- État B : arrêt intermédiaire (diphasique[1]),
- État C : primaire refroidi par le RRA (refroidissement du réacteur à l'arrêt),
- État D : circuit primaire ouvert.

Avec les EPS, on peut calculer des risques par état, qu'on notera $R|_{Et.k}$ pour l'état k. Il est à noter que [85] :

$$R = R|_{Et.A} + R|_{Et.B} + R|_{Et.C} + R|_{Et.D}$$

A partir de ces différentes notations, on peut définir :

$R_{CL_j}\big|_{Et.\,k}$ le risque lorsque l'on est dans l'état k et que l'événement CL_j est certain : $P\left(CI/CL_j\right)|_{Et.\,k}$

$R_{E_i}|_{Et.\,k}$ le risque lorsque l'on est dans l'état k et que l'événement E_i est certain : $P\left(CI/E_i\right)|_{Et.\,k}$

$R_{CL_j;E_i}\big|_{Et.\,k}$ le risque lorsque l'on est dans l'état k et que l'événement CL_j et l'événement E_i sont certains : $P\left(CI/CL_j \cap E_i\right)|_{Et.\,k}$

Calcul du risque sachant une condition limite ou un cumul : Dans le cas d'une condition limite, l'indisponibilité d'un composant ou d'un sous-système est provoquée. On sait quels sont les EB réalisés. On pourra donc calculer $R_{CL_j}\big|_{Et.\,k}$ au moyen d'un groupe PGT incluant les EB certains. On a alors :

$$R_{CL_j}\big|_{Et.\,k} = P\left(CI/E_{1;PGT_{CL_j}}\right)\Big|_{Et.\,k}$$

Dans le cas d'un événement de groupe 1 fortuit, si on a précisément diagnostiqué la panne, on sait quels EB sont réalisés et, dans ce cas, l'événement de groupe 1 est modélisé au moyen d'un groupe PGT pour calculer $R_{E_i}|_{Et.\,k}$. Si on ne sait pas précisément quel matériel a provoqué l'occurrence de l'événement de groupe 1, on peut utiliser une démarche de type "importance d'un système" (c.f. section 1.2 de ce chapitre). Pour ce faire, il faut modéliser l'occurrence de l'événement de groupe 1 considéré en prenant en compte les matériels que l'on sait non défaillants.

[1]Le circuit primaire est refroidi par les générateurs de vapeur qui produisent de la vapeur, le circuit secondaire est donc diphasique.

Par exemple, si on considère un événement de groupe 1 fortuit qui correspond à la perte de la voie A de l'ISHP (c.f. figure 3.1), on modélisera cette perte comme étant due à la défaillance de la vanne 1, ou à la défaillance de la pompe 1, ou encore à une perte d'alimentation électrique locale, mais ni à la maintenance de la pompe 1 (on sait qu'il n'y a pas de maintenance en cours) ni à une perte généralisée de l'alimentation électrique de la voie A (pas de panne signalée en salle de commande). L'occurrence de l'événement de groupe 1 "perte d'une voie de l'ISHP" est modélisée au moyen de l'arbre de défaillances de la figure 3.12. Dans cet arbre, ni les pertes électriques ni la maintenance ne sont modélisées.

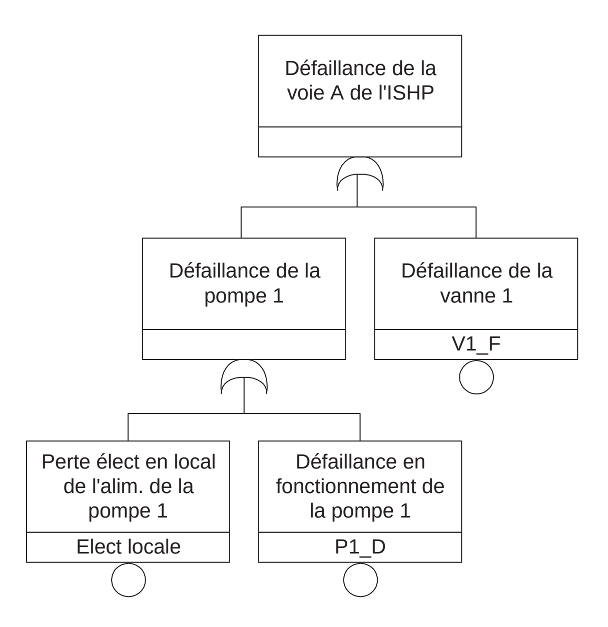


FIG. 3.12 – *Modélisation de l'événement de groupe 1 "perte de la voie A de l'ISHP"*

Ensuite, pour calculer $R_{E_i}|_{Et.\ k}$, on utilise cet arbre de défaillances comme indiqué dans la section 1.6.1 de ce chapitre en considérant que :

$$R_{E_i}|_{Et.\ k} = \left.\frac{P\left(CI \cap E_i\right)}{P\left(E_i\right)}\right|_{Et.\ k}$$

2.2.2 Pourquoi les mesures d'importance classiques sont inadaptées

Le but est d'utiliser ou de définir des indicateurs de risque qui permettent de distinguer les cumuls ayant un fort impact sur le risque de ceux en ayant un moins important. Pour chaque condition limite, on considérera donc l'accroissement de risque consécutif à l'occurrence de chaque événement de groupe 1 relativement à un état donné.

La solution la plus simple pourrait être de calculer les FAR et les FDR des événements du groupe 1 sachant l'existence d'une condition limite j. Cette démarche n'est pas pertinente car de nombreux FAR et FDR sont élevés "dans l'absolu", que l'événement j soit réalisé ou non. Dans ce cas, des mesures pour prévenir leur défaillance ou assurer leur fiabilité sont déjà définies dans le cadre de l'exploitation générale et elles n'ont pas à être modifiées à cause de l'existence d'une condition limite. Pour supprimer les événements correspondant à des FAR et des FDR élevés "dans l'absolu", on pourrait comparer pour chaque matériel la variation de son FAR et de son FDR lorsqu'on a une condition limite et lorsqu'on ne l'a pas. On pourrait penser que si le FAR d'un matériel augmente lors d'une condition limite, cela signifierait que ce matériel et ceux faisant l'objet de la condition limite interviennent dans les mêmes séquences accidentelles. On pourrait aussi penser, à tort, que si les mesures d'importance ne varient pas, l'importance

du matériel ne varie pas, qu'il y ait ou non une condition limite j. Or, ce n'est pas le cas. En effet, supposons que :

$$\left.\overbrace{\left(P\left(CI/E_i \cap CL_j\right) - P\left(CI/CL_j\right)\right)}^{\text{accroissement de risque dû à } E_i \text{ sachant } CL_j} - \overbrace{\left(P\left(CI/E_i\right) - P\left(CI\right)\right)}^{\text{accroissement de risque dû à } E_i}\right|_{Et.\ k} = 0 \quad (3.2)$$

Ceci revient à dire que l'accroissement de risque consécutif à l'occurrence de l'événement de groupe 1 E_i reste le même, que j soit indisponible ou non (que j fasse, ou non, l'objet d'une condition limite). Dans ce cas, le cumul de E_i et de CL_j n'est pas très préjudiciable vu que ces deux événements ne sont pas liés (pas contenus dans les mêmes coupes). Pourtant, le FAR de i sachant l'indisponibilité de j n'est pas le même que le FAR dans l'état de référence car :

$$FAR_{indispo\ j}\left(E_i\right)\big|_{Et.\ k} - FAR_{etat\ de\ ref.}\left(E_i\right)\big|_{Et.\ k} =$$

$$\frac{P\left(CI/E_i \cap CL_j\right) - P\left(CI/E_j\right)}{P\left(CI/CL_j\right)} - \frac{P\left(CI/E_i\right) - P\left(CI\right)}{P\left(CI\right)}$$

Même si les numérateurs sont identiques (hypothèse de l'équation 3.2), le dénominateur du FAR sachant l'indisponibilité de j est supérieur à celui du FAR sachant que j est dans son état de référence. Donc sous l'hypothèse 3.2 :

$$FAR_{indispo\ j}\left(E_i\right)\big|_{Et.\ k} < FAR_{etat\ de\ ref.}\left(E_i\right)\big|_{Et.\ k}$$

Il en est de même pour le FDR. Même si la probabilité d'être dans un état pour lequel i est critique et en panne reste inchangée, qu'on ait ou non une condition limite sur j, la valeur du FDR changera néanmoins. En effet, le numérateur du FDR reste le même, mais pas le dénominateur. On aura donc :

$$FDR_{indispo\ j}\left(E_i\right)\big|_{Et.\ k} < FDR_{etat\ de\ ref.}\left(E_i\right)\big|_{Et.\ k}$$

On ne peut donc pas faire reposer le processus d'identification des cumuls correspondant à un gros accroissement de risque sur la comparaison des facteurs d'importance dans l'état de référence et leur valeur sachant l'indisponibilité de j.

2.2.3 Valeurs à mesurer dans le cas des cumuls

Parmi les événements considérés, on s'intéresse plus particulièrement [100] :

- à ceux qui contribuent le plus au risque, c'est-à-dire ceux qui, s'ils ne pouvaient pas se produire, impliqueraient la plus grande baisse du niveau de risque ou, formulé encore autrement, aux événements i pour lesquels la probabilité que la tranche soit dans un état où i est critique et réalisé soit la plus grande (l'occurrence de i a provoqué l'occurrence de conséquences inacceptables),
- et à ceux qui contribuent le plus à la sûreté, c'est-à-dire à ceux qui garantissent que le niveau du risque de référence est bas ou, formulé autrement, à ceux qui, si leur occurrence était certaine, impliqueraient la plus grosse augmentation de risque.

Dans le cadre de la gestion des cumuls, on veut savoir quel sont les événements de groupe 1 dont la contribution au risque ou la contribution à la sûreté s'accroît très fortement lorsqu'une condition limite existe.

Ainsi, pour chaque condition limite CL_j considérée sur un état donné $Et.\ k$, on veut savoir, pour chaque événement E_i de groupe 1, si sa contribution au risque varie significativement du fait de la condition limite CL_j.

2.2.4 Apprécier la variation de la contribution à la sûreté : Le Facteur d'Accroissement de Risque Potentiel (FARP)

L'objectif est de mesurer l'accroissement de la contribution à la sûreté d'un événement E_i lorsqu'un événement E_j se produit.

Pour étudier la contribution à la sûreté du cumul de deux macro-événements E_i et E_j, nous avons défini le Facteur d'Accroissement de Risque Potentiel (FARP) comme *L'accroissement de la contribution à la sûreté d'un événement E_i lorsqu'un événement E_j est certain, pondéré par le risque de référence. On peut plus simplement dire que le FARP du binôme E_i/E_j correspond à l'augmentation de la probabilité, quand E_j est certain, que E_i soit critique mais qu'il ne se produise pas, pondérée par le risque de référence.*

$$
\begin{aligned}
FARP\,(E_i/E_j) &= FARP\,(E_j/E_i) \\
&= \frac{(R_{i,1}-R)_{indispo.\ j} - (R_{i,1}-R)_{etat\ ref}}{R} \\
&= \frac{(P\,(CI/E_i \cap E_j) - P\,(CI/E_j)) - (P\,(CI/E_i) - P\,(CI))}{P\,(CI)} \\
&= \frac{R_{indispo.\ j} \cdot (FAR\,(E_i))_{indispo.\ j} - R \cdot (FAR\,(E_i))_{etat\ ref}}{R}
\end{aligned}
$$

Sous réserve que le modèle employé soit cohérent et en se souvenant que dans ce cas, $P\,(CI/E_i) - P\left(CI/\overline{E_i}\right) = P\,(E_i\ est\ critique)$, on peut dire que :

$$FARP\,(E_i/E_j) = \frac{(1-P\,(E_i)) \cdot (P\,(E_i\ est\ critique/E_j) - P\,(E_i\ est\ critique))}{R}$$

avec $P\,(E_i\ est\ critique/E_j)$ la probabilité que la tranche soit dans un état critique relativement à l'événement E_i lorsque l'événement E_j est certain.

Le FARP est à valeur dans $\left[-FAR\,(E_i)|_{etat\ ref.}\,;\,\frac{1}{R}\right]$. La borne inférieure est atteinte lorsque l'événement i ne peut plus être critique lorsque la condition limite j est avérée. C'est par exemple le cas pour des systèmes en série. Si l'événement E_i et l'événement E_j correspondent aux défaillances des matériels (ou systèmes) i et j et que ces matériels (ou systèmes) sont fonctionnellement en série, l'arrêt du matériel j, dû à une condition limite, rend inutile le matériel i. Sa défaillance n'a alors aucun impact sur le risque. On a donc $(R_{i,1}-R)_{indispo.\ j} = 0$. La borne supérieure est atteinte lorsqu'un événement i, ayant une probabilité d'occurrence nulle, jamais critique dans le cadre de référence, le devient tout le temps lorsqu'il y a une condition limite portant sur un événement j. Ce cas de figure est assez hypothétique. Il s'agit d'une borne qu'on peut ne pas forcément atteindre.

2.2.5 Apprécier la variation de la contribution au risque : le Facteur d'Accroissement de Contribution au Risque (FACR)

L'objectif est de mesurer l'accroissement de la contribution au risque d'un événement E_i lorsqu'un événement E_j se produit.

Pour étudier la contribution au risque du cumul de deux événements, nous avons défini le Facteur d'Accroissement de Contribution au Risque (FACR) comme *L'accroissement de la contribution au risque d'un événement E_i lorsqu'un événement E_j est certain, pondéré par le risque de référence. Cette mesure peut être relative à un état de la centrale. Exprimé différemment, le FACR traduit l'augmentation de la probabilité, lorsque l'événement E_j est certain, que l'occurrence de l'événement E_i entraîne l'occurrence de l'événement CI, pondérée par le risque de référence. On peut plus simplement dire que le FACR du binôme E_i/E_j correspond à l'augmentation de la probabilité, quand E_j est certain, que E_i soit critique et qu'il se produise, pondérée par le risque de référence.*

$$\begin{aligned} FACR\,(E_i/E_j) &= FACR\,(E_j/E_i) \\ &= \frac{(R-R_{i,0})_{indispo.\;j}-(R-R_{i,0})_{etat\;ref}}{R} \\ &= \frac{\left(P\,(CI/E_j)-P\left(CI/\overline{E_i}\cap E_j\right)\right)-\left(P\,(CI)-P\left(CI/\overline{E_i}\right)\right)}{P\,(CI)} \\ &= \frac{R_{indispo.\;j}\cdot(FDR\,(E_i))_{indispo.\;j}-R\cdot(FDR\,(E_i))_{etat\;ref}}{R} \end{aligned}$$

Sous réserve que le modèle utilisé pour calculer les FACR soit cohérent, on obtient :

$$FACR\,(E_i/E_j) = \frac{P\,(E_i)\cdot(P\,(E_i\;est\;critique/E_j)-P\,(E_i\;est\;critique))}{R}$$

avec $P\,(E_i\;est\;critique/E_j)$ la probabilité que la tranche soit dans un état critique relativement à l'événement E_i.

Le FACR est à valeur dans $\left[-FDR\,(E_i)|_{etat\;ref.}\,;\,\frac{1}{R}\right]$. De même que pour le FARP, la borne inférieure est atteinte lorsqu'un événement E_j, ne peut plus être critique lorsque la condition limite correspondant à la réalisation de l'événement E_j est en cours. La borne supérieure est atteinte lorsqu'un événement i, ayant une probabilité d'occurrence de 1, jamais critique dans le cadre de référence, le devient tout le temps lorsqu'il y a une condition limite portant sur un événement j. Ce cas de figure est assez hypothétique. Il s'agit d'une borne qu'on peut ne pas forcément atteindre.

2.3 Mise en œuvre de ces indicateurs

Le but de cette section est de voir comment les facteurs que nous venons de définir peuvent être employés pour la gestion des cumuls d'indisponibilité. Pour ce faire, nous allons voir comment on peut les calculer et les interpréter.

2.3.1 Comment calculer FARP et FACR dans le cas des cumuls d'indisponibilité

Comme on l'a vu dans la section 2.2.1 de ce chapitre, une condition limite CL_i correspond en général à l'occurrence certaine de l'événement PGT $E_{1;PGT_{CL_i}}$. L'occurrence fortuite et concomitante d'un autre événement de groupe 1 correspond en revanche le plus souvent à l'occurrence d'un événement exprimé au moyen d'un arbre de défaillances.

Donc bien que pour le FARP comme pour le FACR, on ait :

$$FARP\,(E_i/E_j) = FARP\,(E_j/E_i) \text{ et } FACR\,(E_i/E_j) = FACR\,(E_j/E_i)\,,$$

le calcul du FACR ou du FARP de l'événement fortuit i de groupe 1, noté E_i, sachant l'existence d'une condition limite sur l'événement j de groupe 1, noté E_{CL_j}, n'est pas le même que lorsque la condition limite porte sur i et que l'événement fortuit est j. Ainsi, $FARP\left(E_i/E_{CL_j}\right) = FARP\left(E_{CL_j}/E_i\right) \neq FARP\,(E_j/E_{CL_i})$

Quand on a une condition limite sur l'événement j et qu'on considère l'occurrence fortuite de E_i, on calculera :

$$FARP\left(E_{syst.i}/E_{1;PGT_j}\right) \text{ et } FACR\left(E_{syst.i}/E_{1;PGT_j}\right)$$

avec :

$E_{syst.i}$ l'événement de groupe 1 fortuit correspondant à une défaillance de cause inconnue d'un composant ou d'un sous-système ;

$E_{1;PGT_j}$ l'événement "occurrence simultanée de tous les EB du groupe PGT", qui contient les événements certains lors de la condition limite.

2.3.2 *Interprétation des résultats de ces facteurs*

Utilisation du FARP

On peut noter que le FARP équivaut à la variation de risque lorsque E_i et E_j sont certains, à laquelle on soustrait la somme des variations de risque lorsque E_i seul est certain et lorsque E_j seul est certain :

$$FARP\,(E_i/E_j) =$$
$$= \frac{\overbrace{(P\,(CI/E_i \cap E_j) - P\,(CI))}^{\Delta_{R_{i,j,1}}} - \overbrace{(P\,(CI/E_i) - P\,(CI))}^{\Delta_{R_{i,1}}} - \overbrace{(P\,(CI/E_j) - P\,(CI))}^{\Delta_{R_{j,1}}}}{P\,(CI)}$$

Si le FARP est positif et significativement différent de zéro : Alors i et j sont (au moins partiellement) fonctionnellement redondants. Ils interviennent dans les mêmes séquences accidentelles. Si le FARP est très supérieur à zéro, la défaillance de i sachant que j fait l'objet d'une indisponibilité programmée implique une augmentation de risque bien supérieure à ce qu'elle serait si j était dans son état de référence. L'augmentation de risque consécutive à l'occurrence de E_i et E_j est supérieure à la somme de l'augmentation de risque consécutive à l'occurrence de E_i et de celle consécutive à l'occurrence de E_j. En termes de prévention de risque, il faut, lorsque la condition limite j est avérée, prévenir la défaillance ou l'indisponibilité de i. Des mesures spécifiques pour prévenir la défaillance de i sont définies lorsque la condition limite j est avérée.

On parle alors d'un cumul d'événements ayant un **effet "amplificateur"**. Ce terme permet de souligner que l'impact sur le risque de l'occurrence de ces deux événements est bien supérieur à la somme des impacts de chaque événement considéré indépendamment.

Si le FARP est proche de zéro : Alors i et j sont fonctionnellement indépendants, ils n'interviennent pas dans les mêmes séquences accidentelles. L'augmentation de risque consécutive à l'occurrence de E_i et E_j est égale à la somme de l'augmentation de risque consécutive à l'occurrence de E_i et de celle consécutive à l'occurrence de E_j. En termes de prévention de risque (définition des mesures palliatives de E_j notamment), on peut traiter ces deux indisponibilités indépendamment. Il n'y aura pas de mesure spécifique portant sur i pour pallier l'indisponibilité de j. Lorsque E_j est avéré, aucune mesure ne doit être prise concernant i.

On parle alors d'un cumul d'événements ayant un **effet "additif"**. Ce terme permet de souligner que l'impact sur le risque de l'occurrence de ces deux événements est équivalent à la somme des impacts de chaque événement considéré indépendamment.

Si le FARP est négatif : Alors i et j sont au moins partiellement fonctionnellement en série. Si j est défaillant, alors i est moins sollicité et la probabilité que E_i soit critique décroît. En termes de prévention de risque, aucune mesure pour pallier l'occurrence provoquée de E_j ne doit porter sur i car l'importance de i pour la sûreté a décru.

Dans le cas particulier où $FARP\,(E_i) = -FAR\,(E_i)$, les matériels i et j sont fonctionnellement totalement en série. Si l'événement E_j est certain, l'occurrence de l'événement E_i n'a plus aucun impact sur le risque.

Dans ce dernier cas ($FARP\,(E_i) = -FAR\,(E_i)$), on parle d'un cumul d'événements ayant un **effet "nul"**. Ce terme permet de souligner que l'impact sur le risque de l'occurrence de ces deux événements est égal à l'impact de l'un ou de l'autre de ces deux événements considérés indépendamment.

Utilisation du FACR

Si le FACR est positif et significativement différent de zéro : Cela veut dire que la probabilité que l'occurrence de E_i provoque l'occurrence de l'événement CI sachant l'occurrence de E_j est plus élevée que la probabilité que la défaillance de i provoque l'occurrence de l'événement CI lorsque j est dans son état de référence. Dans ce cas, i et j sont (au moins partiellement) fonctionnellement redondants. Ils interviennent dans les mêmes séquences accidentelles. En termes de contrôle du risque, il faut, lorsque la condition limite j est avérée, chercher à fiabiliser i. Pour ce faire, on peut définir des mesures ponctuelles qui reviennent à fiabiliser i ou à diminuer son importance (ajout de redondances par exemple) avant de provoquer une condition limite sur j.

Si le FACR est proche de zéro : Alors i et j sont fonctionnellement indépendants, ils n'interviennent pas dans les mêmes séquences accidentelles. En termes de contrôle du risque (définition des mesures palliatives de E_j notamment), on peut traiter ces deux indisponibilités indépendamment. Il n'y aura pas de mesure spécifique portant sur i pour pallier l'indisponibilité de j. Lorsque E_j est avéré, aucune mesure spécifique ne doit être prise concernant i car la contribution de E_i au risque reste inchangée.

Si le FACR est négatif et significativement différent de zéro : Alors i et j sont au moins partiellement fonctionnellement en série. Si j est défaillant, alors i est moins sollicité et la probabilité que E_i soit critique décroît. En termes de contrôle du risque, aucune mesure pour pallier à l'occurrence provoquée de E_j ne doit porter sur i car la contribution de i au risque a décru.
Dans le cas particulier où $FACR\,(E_i) = -FDR\,(E_i)$, les matériels i et j sont fonctionnellement totalement en série. Si l'événement E_j est certain, l'occurrence de l'événement E_i n'a plus aucun impact sur le risque.

Exemple : On étudie le schéma 3.13. Dans cet exemple, l'événement CI est la non-arrivée du fluide. Les événements considérés sont ceux du tableau 3.3.

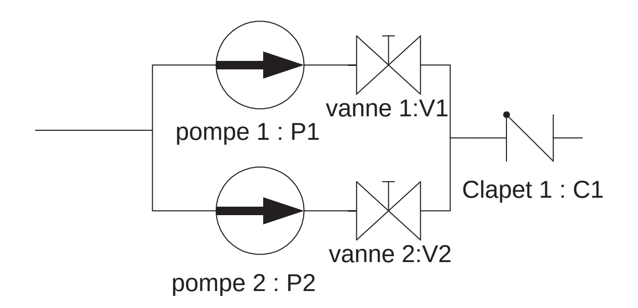


FIG. 3.13 – *Système étudié*

Nom de l'événement	probabilité d'occurence	Description
P_1	10^{-3}	Défaillance de la pompe 1
P_2	10^{-3}	Défaillance de la pompe 2
V_1	10^{-6}	fermeture intempestive de la vanne 1
V_2	10^{-6}	fermeture intempestive de la vanne 2
C_1	10^{-8}	blocage fermé du clapet 1

TAB. 3.3 – *Données sur les composants de l'exemple*

Avec ces données, on trouve $P(CI) = 1.012 \cdot 10^{-6}$. On provoque l'indisponibilité de la pompe 1. On trouve $P(CI/P_1) = 1.00101 \cdot 10^{-3}$. On obtient alors les résultats du tableau 3.4.

Événement	$FAR_{etat\ ref}$	$FDR_{etat\ ref}$	$FARP_{/P_1}$	$FACR_{/P_1}$
P_1	988	0.99	Pas de FAR calc. pour un événement certain	
P_2	988	0.99	$9,86 \cdot 10^5$	987
V_1	988	$9.88 \cdot 10^{-4}$	-988	$-9.88 \cdot 10^{-4}$
V_2	988	$9.88 \cdot 10^{-4}$	$9.87 \cdot 10^5$	0.987
C_1	$9.88 \cdot 10^5$	$9.88 \cdot 10^{-3}$	0	0

TAB. 3.4 – *Facteurs d'importance calculés*

Avec les résultats du tableau 3.4, on vérifie que :
- $FARP(C_1/P_1) = FACR(C_1/P_1) = 0$. En effet, le matériel C_1 est toujours critique et ni son importance ni sa contribution au risque ne varient quand on provoque l'indisponibilité de la pompe 1.
- Le FARP et le FACR de la pompe 2 sont très élevés. En effet, quand la pompe 1 est indisponible, la pompe 2 devient critique. Son FARP est donc très élevé. De plus, l'événement P_2 est relativement probable si on le compare aux autres. Son FACR est donc élevé. Le fait que FARP et FACR soient supérieurs à zéro traduit bien une redondance fonctionnelle (au moins partielle et même totale dans notre cas) avec la pompe 1.
- Le FARP de la vanne 2 est très élevé (et presque égal à $FARP(P_2/P_1)$). Cela s'explique par le fait que lors de l'indisponibilité de la pompe 1, la vanne 2 est toujours critique. Son FACR, en revanche, est faible si on le compare à celui de la pompe 2 car la probabilité de défaillance de la vanne 2 est faible (10^{-6}).
- Pour la vanne 1, son FARP est égal à moins son FAR dans l'état de référence et son FACR est égal à moins son FDR dans l'état de référence car la probabilité que la vanne 1 soit critique est nulle lorsque la pompe 1 fait l'objet d'une condition limite. Elle n'est plus sollicitée. Cela traduit bien le fait que la pompe 1 et la vanne 1 sont fonctionnellement en série.

2.4 Application de ces indicateurs

La réflexion sur les cumuls d'événements de groupe 1 menée dans le cadre de cette thèse a abouti à une proposition de méthode pour la modification des règles définissant les délais de repli. Cette proposition a pris la forme d'une note technique intitulée "*Méthode EPS de gestion des cumuls d'indisponibilité appliquée aux conditions limites et première application*" [85] et transmise au centre d'ingénierie d'EDF.

Cette note développe différentes propositions de démarche de modification des délais de repli en cas de cumul d'une condition limite et d'un événement de groupe 1 fortuit.

La première consiste à faire évoluer la démarche actuelle en définissant les délais de repli en l'absence de cumul au moyen des EPS, puis, en cas de cumul, en gardant la règle existante (décrite dans la section 2.1 de ce chapitre).

La deuxième se fonde sur une démarche en plusieurs étapes. On calcule tout d'abord $R_{CL_j;E_i}\big|_{Et \cdot k}$ (le risque sachant l'événement fortuit E_i alors qu'une condition limite CL_j est en cours, le tout considéré sur un état k). Si ce risque est trop important (>10^{-7}), dès l'occurrence de l'événement fortuit E_i de groupe 1 alors que la condition limite CL_j est en cours, le repli doit être immédiat (avant 1 heure).

Si ce n'est pas le cas, on calcule le FARP de E_i/CL_j.

- Si ce FARP est négatif ou nul, on est face à un cumul dit "additif", les limitations de délai

restent celles associées à ces deux événements lorsqu'on les considère hors cumul. C'est à dire que chaque condition limite doit être traitée comme si le cumul n'existait pas (l'une et l'autre doivent être levées avant leurs délais respectifs).
- Sinon, on définit un nouveau délai à partir de $\left(R_{CL_j;E_i}\big|_{Et.k} - R\big|_{Et.k}\right)$ et de l'accroissement de risque acceptable, qui est de 10^{-7} (pour plus d'informations sur ce calcul, se référer à [85]) .

Dans [85], on peut lire que "*l'avantage de cette* [seconde] *démarche est de proposer une gestion plus adaptée de chaque cumul. Elle pourrait s'appliquer également au traitement des cumuls pour d'autres types d'indisponibilités programmées (par exemple, les indisponibilités générées par les Essais Périodiques). Son inconvénient est la nécessité de faire un traitement a priori de tous les cumuls deux à deux, pour chaque condition limite étudiée. Cela implique, même si le calcul peut être automatisé, une charge de travail supplémentaire, mais surtout, cela conduit à un référentiel plus complexe pour l'exploitant*".

Cette alternative à la gestion actuelle des cumuls, basée sur le fait qu'on recherche si l'effet des deux événements de groupe 1 est "amplificateur" ou "additif", peut être rapprochée de la démarche mise en œuvre par la Duke Power Company [35] qui, sans définir d'indicateurs tels que le FARP, compare la somme des FAR de chaque événement de groupe 1 considéré séparément au FAR du groupe PGT contenant ces deux événements.

Pour permettre le calcul des FARP, nous avons adapté le prototype de l'application SENSIB (c.f. §2.2.2 du chapitre 2). Il permet maintenant le calcul de FARP et des FACR pour chaque événement de base sachant une condition limite donnée (modélisée au moyen d'un groupe PGT). Cette application ne permet pas encore le calcul de FARP ou de FACR pour des événements fortuits de groupe 1 exprimés au moyen d'arbres de défaillances (comme proposé dans la section 2.2.1 de ce chapitre).

3 Conclusion sur la définition et l'utilisation de mesures d'importance étendues

Notre objectif initial était de proposer des mesures d'importance "étendues" à d'autres niveaux que le seul niveau des événements de base. Pour l'atteindre, nous avons dû clarifier quels pouvaient être ces niveaux :
- un groupe d'EB, défini par des critères géographiques, techniques ou physiques,
- un système défini par une fonction (telle que fournir de l'eau à un débit, sur une durée et à une pression donnés),
- une fonction en ne considérant que son existence ou sa non-existence (et non pas le fonctionnement ou la défaillance du système qui la supporte).

Cette clarification avait pour but de permettre de nouvelles applications. La gestion des délais avant de replier la tranche en cas de cumul d'événements de groupe 1 n'est qu'une application concrète de ce que permettent ces mesures d'importance étendues. La mise en œuvre effective de cette démarche à EDF (elle n'est pour l'instant pas encore adoptée) serait la première application concrète du calcul de mesures d'importance au niveau d'un système. De nombreuses autres nouvelles applications peuvent être développées en employant ces mesures "étendues", notamment l'aide à la conception, ainsi que nous l'exposons dans le chapitre suivant.

Chapitre 4

Des indicateurs de risque comme outils d'aide à la conception

Lors de la conception d'une nouvelle centrale nucléaire, des lignes de défense sont créées pour prévenir ou mitiger les conséquences d'un événement perturbateur. Afin de garantir un niveau de risque acceptable, plusieurs lignes de défense indépendantes doivent s'interposer entre un événement perturbateur et l'atteinte de conséquences inacceptables. Pour éviter que le coût de construction et d'exploitation soit trop élevé, il faut que ces lignes de défense ne soient pas surnuméraires. L'objectif de la conception d'une centrale est donc de s'assurer de la bonne couverture de tous les risques, de la robustesse de l'installation face à des événements perturbateurs, sans pour autant la sur-protéger contre certains risques. Dans ce chapitre, nous proposons une démarche de conception, basée sur une approche de type "EPS à la conception", qui permet de vérifier la bonne répartition et l'indépendance des lignes de défense.

La première partie de ce chapitre présente notre définition d'une ligne de défense, ainsi que la manière de la modéliser dans une EPS de conception. La seconde partie vise à exposer notre démarche d'aide à la création et à la répartition des lignes de défense. Dans la troisième partie enfin sont proposés d'autres outils pour vérifier leur indépendance et, le cas échéant, traiter les modes communs fonctionnels entre plusieurs lignes de défense impliquées dans une même trajectoire accidentelle.

L'approche que nous développons dans ce chapitre n'est qu'une ébauche de ce que pourrait être une démarche de conception. Cette approche n'a été rédigée que pour pouvoir servir de première base à une discussion sur l'utilisation conjointe de la démarche déterministe et de la démarche probabiliste. Il ne s'agit pas d'une méthode "clef en main".

1 Contexte de l'étude

1.1 *Définitions*

Rappels

Dans la littérature internationale sont utilisés des termes tels que "*barrière physique*", "*fonction de sûreté*", "*fonction d'une barrière*", "*système d'une barrière*" et "*ligne de défense*" [80, 34, 57, 61, 97, 60]. Pour éviter toute ambiguïté sur ces termes, nous rappelons leur définition avant toute utilisation de ces concepts.

Le Memento de la sûreté nucléaire [39] propose la définition suivante du terme barrière : "*des obstacles physiques à la dispersion des produits radioactifs*". Dans les centrales actuelles, il existe trois barrières physiques : la gaine du combustible, le circuit primaire et l'enceinte de confinement. Le terme "barrière" ou encore "barrière physique" sera réservé à la désignation de

ces "*obstacles physiques*".

Le terme "fonction de sûreté" sera réservé à la désignation des trois fonctions de sûreté [39] : maîtriser la réactivité, refroidir le combustible et confiner les produits radioactifs. Pour de nouveaux types de centrale, on peut imaginer que ces fonctions soient légèrement différentes, mais dans tous les cas, le terme "fonction de sûreté" sera réservé, dans cette thèse, à la désignation de quelques fonctions essentielles dont la perte de l'une d'elles entraîne l'atteinte de conséquences inacceptables.

Pour définir les termes "barrière de sûreté", "fonction barrière" et "système barrière", nous nous reportons à [80]. Une barrière de sûreté est définie comme un "*un moyen, physique ou immatériel* [une procédure, une "bonne pratique", etc.] *conçu pour prévenir, contrôler ou limiter les conséquences d'un accident*" , une fonction barrière est "*une fonction conçue pour prévenir, contrôler ou limiter les conséquences d'un accident*" et enfin un système barrière est "*un système qui a été conçu pour remplir une ou plusieurs fonctions barrière*".

Même si les barrières de sûreté peuvent être classifiées comme participant à la "*prévention*", au "*contrôle*" et à la "*mitigation*" d'un accident [80], de manière générale, dans les modèles EPS, ce sont uniquement les barrières de sûreté dédiées au contrôle qui sont explicitement prises en compte. Les barrières de sûreté liées à la prévention[1] ainsi que celles liées à la mitigation[2] ne sont en revanche pas complètement modélisées.

Ligne de défense

Pour définir ce qu'est une ligne de défense, nous regroupons les notions de barrière de sûreté, fonction barrière et système barrière. Une ligne de défense correspond à une fonction (la fonction barrière) et à l'ensemble structuré de composants la remplissant (le système barrière). Une ligne de défense est défaillante lorsqu'elle ne remplit plus sa fonction. Dans cette définition de la ligne de défense, un système ne remplit qu'une seule fonction, mais un composant ou un sous-système peut appartenir à plusieurs lignes de défense. En cela, cette définition est homogène à la définition d'un système proposée dans le chapitre 1.5 et dans [31]. Une ligne de défense est donc définie comme : *un système défini par une fonction ayant un "impact direct et significatif" [80] sur la prévention de l'occurrence du ou des événements redoutés. Cette fonction peut être prévue pour prévenir, contrôler ou atténuer les conséquences d'un événement non-désiré.*

La répartition des fonctions (et des systèmes qui y sont associés) entre celles correspondant à des lignes de défense et celles n'étant que des sous-fonctions d'autres lignes de défense est pour partie subjective. Un des critères utilisables pour faire cette distinction est la question "Est-ce que cette fonction contribue à la réalisation d'une autre fonction ?". Si la réponse est oui, cette fonction ne correspond probablement pas à une ligne de défense. C'est ainsi le cas des systèmes supports (systèmes électriques, pneumatiques, ventilation, etc.). En effet, bien que le fonctionnement ou le non-fonctionnement de ces systèmes ait un impact fort sur la gestion de nombreux accidents, leur fonction (fournir de l'énergie, refroidir, etc.) contribue à d'autres fonctions, telles que "assurer l'appoint en eau", "refroidir le circuit primaire", etc. Ces systèmes supports sont donc considérés comme des sous-systèmes remplissant des sous-fonctions dans d'autres lignes de défense.

Macro-coupe

Chaque trajectoire accidentelle est décrite comme l'occurrence d'un initiateur et l'échec d'un certain nombre de lignes de défense aboutissant à l'atteinte des conséquences inacceptables (évé-

[1] choix des matériaux, marges, maintenance, inspections, etc.

[2] pour les EPS de niveau 1 : tous les systèmes mis en jeu pour assurer la préservation de l'intégrité des deuxième et troisième barrières physiques, pour les EPS de niveau 2 : les plans particuliers d'intervention tels que l'évacuation des populations, etc.

nement CI). Sous l'hypothèse que la centrale à l'étude a un fonctionnement cohérent (cf. section 2.1.2 chapitre 1), on peut décrire toutes les séquences accidentelles au moyen de macro-coupes. Ces macro-coupes sont des coupes minimales qui s'expriment à partir de macro-événements correspondant à l'échec des lignes de défense, et non à partir d'événements élémentaires correspondant à l'occurrence de modes de défaillance spécifiques de composants spécifiques, comme dans le cas des coupes minimales de référence. Nous définissons donc une macro-coupe comme : *un ensemble minimal d'événements dont l'occurrence simultanée entraîne l'occurrence de conséquences inacceptables. Chaque événement de cet ensemble modélise l'occurrence d'un initiateur ou la défaillance d'une ligne de défense (c'est-à-dire que le système "ligne de défense" échoue à remplir sa fonction).*

Défaillances de causes communes fonctionnelles entre lignes de défense

Certaines lignes de défense peuvent partager, entre elles ou avec un initiateur, des composants ou des sous-systèmes. Elles partagent alors les sous-fonctions associées à ces composants ou à ces sous-systèmes. De ce fait, elles ne sont pas indépendantes [96]. Ces interdépendances fonctionnelles de causes internes (par opposition avec les interdépendances "externes" telles que l'inondation ou l'incendie) peuvent aussi être désignées comme étant des causes communes fonctionnelles. En effet, la perte d'une seule de ces sous-fonctions peut conduire à la défiabilisation ou à la perte des lignes de défense qui la partagent, d'où le nom de cause commune (plusieurs lignes de défenses défiabilisées du fait de la même cause) fonctionnelle (par la perte d'une même sous-fonction). La perte ou la défiabilisation de plusieurs lignes de défense du fait de la défaillance d'une sous-fonction ou d'un matériel partagé peuvent aussi être appelées "modes communs fonctionnels".

1.2 Modélisation des lignes de défense

La manière la plus commode de modéliser les lignes de défense semble être de les prendre en compte comme des événements en tête des arbres d'événements (cf. figure 4.1 page 115). Ainsi, lors de l'étude de chaque séquence accidentelle, les analystes pourront raisonner en termes de succès ou d'échec de lignes de défense. Ceci équivaut à construire les trajectoires accidentelles en termes de succès ou d'échec de fonctions. Cette approche nous semble relativement simple et claire.

Si l'on cherche à appliquer cette définition aux EPS de référence actuelles, on doit apporter certaines modifications. En effet, suite à un examen rapide, on peut par exemple se rendre compte qu'aujourd'hui, dans certains arbres d'événements, les systèmes supports sont modélisés indépendamment des lignes de défense qu'ils supportent. On peut alors se poser la question de savoir si la fonction "fournir de l'énergie" est une fonction principale à part entière qui doit être considérée comme une ligne de défense ou si cette fonction est une sous-fonction d'autres lignes de défense. Il faudrait alors modifier lourdement les modèles EPS actuels pour "internaliser" les systèmes supports. De la même manière, certaines fonctions sont modélisées avec plusieurs événements en tête suivant l'état de puissance de la centrale. On est alors en contradiction avec notre préconisation de modélisation, dans laquelle une ligne de défense correspond à un événement en tête. Cependant, le fait que l'application de la méthode proposée aux modèles actuels nécessiterait quelques mesures de transposition ne remet pas en cause l'intérêt intrinsèque de cette méthode, principalement dédiée à la conception de nouvelles centrales. Les modèles de celles-ci n'existent pas encore et pourront donc être développés de telle façon qu'à une ligne de défense corresponde un événement en tête.

1.3 Démarche et règles de conception

Nouveaux critères de défaillance unique

De manière générale, dans l'ensemble de la démarche proposée dans ce chapitre, nous proposons d'utiliser une version modifiée du critère de défaillance unique. Ce faisant, nous nous inspirons des conclusions proposées par Sorensen dans [81]. Ce critère de défaillance unique sera considéré tout d'abord comme un critère de défaillance qualitatif (adaptation de l'approche "*structurelle*" décrite par Sorensen). Il consiste à vérifier que pour tout initiateur considéré comme certain :
- quel que soit le matériel considéré et quel que soit le mode de défaillance considéré, l'occurrence de ce dernier n'entraîne pas l'atteinte de conséquences inacceptables,
- quelle que soit la ligne de défense considérée, la défaillance de cette dernière n'entraîne pas l'atteinte de conséquences inacceptables.

Ce critère de défaillance unique qualitatif peut être traduit de manière probabiliste (adaptation de l'approche "*rationnelle*" décrite par Sorensen). On a alors un critère de défaillance unique quantitatif, défini de la manière suivante :
- quel que soit le matériel considéré, l'accroissement de risque consécutif à sa défaillance doit rester acceptable,
- quelle que soit la ligne de défense considérée, l'accroissement de risque consécutif à sa défaillance doit rester acceptable.

Objectif d'une démarche de conception

L'objectif, lors de la conception d'une centrale, est le suivant : *concevoir, avec des moyens donnés et des objectifs en termes de production donnés, la centrale la plus sûre possible.*

L'un des moyens pour atteindre cet objectif est de garantir une bonne couverture de tous les risques, c'est-à-dire qu'on doit s'assurer que tous les événements potentiellement dangereux ont été identifiés et que les parades adéquates ont été prévues. Il faut donc vérifier que les différentes lignes de défense sont réparties de manière homogène pour garantir une bonne maîtrise de tous les scénarios accidentels. On doit en particulier s'assurer qu'on n'a pas sur-investi dans le traitement de certains types d'accident tout en laissant ailleurs des "trous" en matière de prévention des risques. On doit enfin vérifier que les moyens de protection mis en œuvre ne peuvent pas être défaillants simultanément du fait de modes communs fonctionnels trop importants. En effet, il faut garantir que plusieurs lignes de défense situées sur une trajectoire accidentelle ne puissent pas être simultanément défaillantes suite à l'occurrence d'une même cause.

La démarche proposée dans ce document reprend ce schéma général de conception. Ainsi, on s'assurera d'abord que tous les risques potentiels ont été envisagés et traités, que la répartition des moyens pour parer à ces différents risques est homogène, puis on vérifiera que la conception du système supportant chaque ligne de défense ne crée pas de trou lié à des modes communs impactant plusieurs lignes de défense.

Inscription de notre approche probabiliste dans le processus de conception d'une centrale

Nous préconisons une démarche de conception en quatre étapes, au sein de laquelle s'inscrit notre démarche probabiliste d'aide à la conception et à la répartition des lignes de défense. Ces étapes sont les suivantes :

1. La première étape consiste à établir les principes de base de fonctionnement du réacteur (choix du modérateur, choix du caloporteur, choix du nombre de circuits, etc.). Cette démarche repose sur une approche déterministe qui est hors du cadre de la présente thèse. A la fin de cette étape, on a défini le fonctionnement général de la centrale à

l'étude, la fonction de chaque ligne de défense et ses conditions de fonctionnement (à l'arrêt, en production, etc.). Par contre, les solutions techniques pour mettre en œuvre ces fonctions, c'est-à-dire les systèmes remplissant la fonction chaque ligne de défense, ne sont pas encore clairement définis.

2. La second étape consiste à modéliser cette conception primitive au moyen d'une EPS "compacte" et à l'enrichir. Dans ce modèle compact, toutes les séquences accidentelles sont précisément modélisées dans les arbres d'événements mais la défaillance des systèmes est modélisée très sommairement. Les lignes de défense sont en particulier considérées comme indépendantes. Certaines lignes de défense pourront être créées, d'autres modifiées ou encore supprimées à partir des enseignements tirés de ce modèle.
3. La troisième étape consiste à affiner le schéma général de la centrale issu de la seconde étape en détaillant la conception de chacune des lignes de défense. Cette démarche repose elle aussi sur une approche déterministe qui est hors du cadre de la présente thèse.
4. Durant la dernière étape, le fonctionnement de la centrale à l'étude, affiné dans la précédente étape, est modélisé dans une EPS "complète". A l'aide de cette EPS, la conception de la centrale évolue encore. Ainsi, les lignes de défense trop interdépendantes sont modifiées, l'importance de chaque matériel est vérifiée et les composants inutiles sont supprimés.

Seules les étapes deux et quatre sont présentées dans cette thèse. Les étapes un et trois reposent principalement sur l'application des principes de conception déjà mis en œuvre lors de la conception des précédentes générations de centrales. On peut retrouver ces principes dans les Règles Fondamentales de Sûreté (RFC) ou dans les Règles de Conception et de Construction des centrales nucléaires à eau légère (RCC) [2, 4, 3, 23, 24, ...].

Limites de notre approche probabiliste

La démarche que nous proposons vise à optimiser la conception et la répartition des différentes lignes de défense. C'est une démarche incomplète dans la mesure où elle vise à améliorer les moyen de contrôle d'un accident mais non les moyens de prévention de ses causes. De même, les moyens de mitigation de l'accident ne seront considérés que si le modèle EPS utilisé est un modèle EPS de niveau II ou III.

Cette focalisation sur les moyens de contrôle d'un accident est due au domaine de couverture des EPS. Les EPS ne modélisent que peu ou pas les actions de prévention d'un initiateur tel que la surveillance des installations, leur maintenance, etc. On ne pourra donc pas valoriser l'importance de telles lignes de défense dans le cadre d'une approche basée sur les EPS.

Enfin, la première étape de la démarche de conception (choix du modérateur, choix du caloporteur, choix du nombre de circuits, etc.) est sans doute celle qui a le plus gros impact sur le risque final. Cette étape ne fait pas l'objet de la démarche que nous proposons. Toutefois, une approche probabiliste, qui reste à définir, pourrait certainement contribuer à éclairer les choix fondamentaux qui doivent être faits durant cette phase.

2 Redéfinir les lignes de défense au moyen d'une démarche probabiliste

Comme on l'a vu dans la section précédente, le principe de notre approche est de concevoir et de répartir les lignes de défense en négligeant leurs interdépendances, puis de modéliser plus finement ces lignes de défense pour identifier puis supprimer les modes communs fonctionnels entre elles qui pèsent trop sur le risque ou sur la sûreté. L'étape qui est décrite dans cette partie, "répartition des lignes de défense", est donc la première de ce processus.

Objectifs de la répartition des lignes de défense

La répartition des lignes de défense doit permettre d'atteindre simultanément quatre objectifs d'égale importance.

- Le premier objectif est l'homogénéité de la répartition des lignes de défense, qui garantit que tous les événements pouvant avoir des conséquences graves ont été identifiés et que les moyens de parade adéquats ont été mis en œuvre pour chacun d'eux.
- En second lieu, la répartition doit satisfaire à l'exigence de redondance, c'est-à-dire que les lignes de défense utilisables doivent être en nombre suffisant pour répondre à tous ces événements. Afin d'en minimiser le nombre total, on visera à assurer la meilleure polyvalence possible des lignes de défense.
- Le troisième objectif est celui d'une utilisation optimale des moyens : il s'agit de contrôler que ces derniers ne soient pas sur-investis en partie inutilement pour se prémunir contre certains événements.
- Enfin, le dernier objectif de la répartition des lignes de défense est celui de la prise en compte de l'imprévisible, ce qui revient à considérer la robustesse de la centrale. En effet, on doit aussi pouvoir contrôler les scénarios non-prévus.

Méthode

Dans un premier temps, le modèle EPS compact va être utilisé de manière qualitative. Il ne sera donc pas utile d'attribuer des probabilités aux événements de base modélisant la défaillance des lignes de défense. Cette première analyse qualitative permettra de définir un premier jeu de modifications du design initial. Une fois ces modifications prises en compte dans le modèle compact, celui-ci sera, dans un second temps, utilisé de manière quantitative. A ce stade, une estimation de la probabilité de défaillance de chaque ligne de défense en conditions accidentelles sera nécessaire. Un nouveau jeu de modifications pourra alors être défini.

En résumé, l'étude de la répartition des lignes de défense se fera en deux temps à partir du modèle compact, tout d'abord de manière qualitative, puis de manière quantitative.

2.1 Préalable à la redéfinition des lignes de défense au moyen d'EPS

Avant de pouvoir appliquer les méthodes proposées dans ce document, les principes de base de fonctionnement du réacteur doivent être définis (choix du modérateur, choix du caloporteur, choix du nombre de circuits, etc.). Ensuite, une approche déterministe "haut niveau" est appliquée pour déterminer les systèmes nécessaires au fonctionnement normal et les lignes de défenses nécessaires à la gestion des accidents majorants. Cette approche est dite "haut niveau" car on ne cherche pas à déterminer la conception précise de chaque système. On s'applique seulement à définir la liste des fonctions qui devront être remplies par des systèmes pour permettre le fonctionnement en état normal et la non-atteinte de conséquences inacceptables quel que soit l'accident majorant considéré.

Une fois ce travail effectué, on dispose de manière grossière du schéma général de fonctionnement de la centrale à l'étude et du design de la centrale exprimé en termes de systèmes, de lignes de défense, et non en termes de composants.

On est alors à même de définir la métrique pertinente pour exprimer le risque. En effet, pour de nouveaux types de centrales, des indicateurs tels que la probabilité de fusion du cœur peuvent ne plus avoir de sens (une telle fusion peut ne plus être physiquement possible, par exemple). En outre, on peut imaginer l'utilisation conjointe de plusieurs métriques de risque.

On est alors en mesure de construire un premier modèle EPS, dit modèle compact. La construction de ce modèle compact nécessite, comme pour un modèle conventionnel, de répertorier tous les événements initiateurs pouvant entraîner l'atteinte de conséquences inacceptables, puis d'étudier toutes les séquences accidentelles possibles qui sont exprimées en termes de suc-

cès et d'échec de lignes de défense. Enfin, chaque ligne de défense est modélisée au moyen d'un unique événement de base. C'est en cela que ce modèle est dit compact. Cette modélisation simpliste du système de chaque ligne de défense permet la construction d'un modèle EPS dès les premiers stades de la conception (avant que le fonctionnement de chaque système soit défini). Elle permet de plus des modifications rapides du modèle et la production d'un jeu de coupes où chaque coupe correspond à une macro-coupe. Pour résumer, un modèle compact est un modèle EPS dont :
- chaque initiateur est modélisé avec une valeur point (un unique EB),
- chaque événement en tête modélise une ligne de défense,
- chaque événement en tête est modélisé avec une valeur point (un unique EB),
- chaque coupe est l'expression d'une macro-coupe.

C'est une fois ce modèle construit que l'approche proposée dans ce document peut être appliquée.

Pour aider à l'utilisation de ce modèle, les initiateurs sont regroupés par familles, c'est-à-dire qu'on associe chaque initiateur à l'un des grands types d'initiateurs (brèche sur le circuit primaire, dilution rapide dans le circuit primaire, etc.). En effet, pour chaque grand type d'accident, on crée plusieurs initiateurs. Par exemple, dans les modèles EPS des réacteurs à eau sous pression (REP), la famille des brèches contient des initiateurs différents pour considérer les différentes tailles de brèche possibles dans les différents états du réacteur (puissance, arrêt, à chaud, arrêt à froid, etc.).

Pour aider à la compréhension des modèles EPS, les lignes de défense peuvent être regroupées par fonction de sûreté. Ainsi, dans les REP, l'injection de sécurité qui permet d'ajouter de l'eau dans le circuit primaire d'une centrale contribue à la fonction de sûreté "refroidir le combustible", car cette eau sert au refroidissement.

Dans un stade ultérieur de conception, notre approche utilisera aussi un modèle dit "complet" (par opposition au modèle compact). Ce modèle complet est un modèle où chaque défaillance de ligne de défense et chaque initiateur sont modélisés aussi finement que possible. Le modèle complet représente une évolution du modèle compact dans la mesure où il partage avec lui les mêmes arbres d'événements, mais ses événements en tête et ses initiateurs y sont modélisés avec des arbres de défaillances et non plus uniquement au moyen de simples valeurs point.

Pour différencier un modèle compact d'un modèle complet, nous définissons les notation suivantes :

$Initiateur$ Le macro-événement "occurrence de l'initiateur",

LD_i Le macro-événement "défaillance de la ligne de défense i",

EB_{Init} L'événement de base du modèle compact modélisant le macro-événement "occurrence de l'initiateur",

EB_{LD_i} L'événement de base du modèle compact modélisant le macro-événement "défaillance de la ligne de défense i",

EB_i L'événement de base du modèle complet modélisant l'événement élémentaire i,

$Init_i$ L'événement de base du modèle complet modélisant l'événement élémentaire "occurrence de l'initiateur i".

Dans le modèle complet, seuls les arbres d'événements dont l'initiateur est un événement élémentaire (une brèche par exemple) contiendront un événement $Init_i$, les autres initiateurs seront modélisés au moyen d'un arbre de défaillances. Dans le modèle compact, en revanche, tous les initiateurs seront modélisés au moyen d'un événement de base EB_{init_k} même si l'événement $Initiateur_k$ dépend de nombreux EB.

Exemple : On suppose l'existence de l'arbre d'événements de la figure 4.1 où apparaissent le modèle complet et le modèle compact.

Initiateur	Ligne de défense 1 LD_1	Ligne de défense 2 LD_2	conseq.
$Init_1$	$EB_1 \cup EB_2 \cup (EB_3 \cap EB_4)$	$EB_2 \cup EB_3$	

1	CA
2	CI
3	CI
4	CI

FIG. 4.1 – *Exemple d'arbre d'événements*

Dans l'exemple de la figure 4.1, deux macro-coupes correspondent à cet arbre d'événements :
- $Initiateur \cap LD1$
- $Initiateur \cap LD2$

La quatrième séquence ne produit aucune macro-coupe car la macro-coupe $Initiateur \cap LD1 \cap LD2$ n'est pas minimale. Le modèle compact produit deux coupes qui correspondent à ces macro-coupes :
- $EB_{Init} \cap EB_{LD1}$
- $EB_{Init} \cap EB_{LD2}$

Le modèle complet de cet arbre d'événements produit trois coupes minimales :
- $Init_1 \cap EB_1$
- $Init_1 \cap EB_2$
- $Init_1 \cap EB_3$

2.2 Approche qualitative de la redéfinition des lignes de défense

Cette section décrit une approche de conception qui utilise des méthodes à la croisée entre analyse fonctionnelle, analyse de la valeur et sûreté de fonctionnement. Elle décrit un processus de conception dont les méthodes n'appartiennent pas réellement à la famille des indicateurs de risque qui font l'objet de cette thèse. Nous jugeons tout de même utile de la présenter pour permettre au lecteur d'avoir une vision générale de l'utilisation des EPS que nous préconisons pour la conception d'une centrale et pour lui permettre de comprendre où se situent, dans la démarche de conception, les indicateurs de risque que nous proposons.

2.2.1 Objectif "qualitatifs" à atteindre pour garantir une conception sûre à moindre coût

Pour garantir un niveau de sûreté acceptable à plus bas coût, la centrale nucléaire que l'on conçoit doit répondre aux deux critères suivants : elle doit être simple et robuste.

La simplicité de la conception de la centrale doit se comprendre sous plusieurs axes. L'évolution des paramètres physiques et techniques conditionnant l'atteinte de conséquences inacceptables doit être la plus simple et la plus lente possible. Ainsi, l'impact de chaque ligne de défense sur l'accident, sur ses paramètres physiques, etc., ainsi que sur les autres lignes de défense, doit être simple quel que soit le contexte. Alors l'action sur le système global "centrale nucléaire" de chaque ligne de défense, ainsi que l'impact de leur défaillance éventuelle, sera intelligible par les équipes de conduite [72]. De plus, le diagnostic d'une éventuelle panne sera facilité. Il en résultera une diminution du risque lié aux actions humaines.

Le design de la centrale doit être le plus simple possible. Pour des objectifs en termes de sûreté, de défense en profondeur et de disponibilité donnés, le nombre de systèmes, d'initiateurs

pouvant affecter le fonctionnement de la centrale, de matériels au sein de chaque système, etc., doit être le plus limité possible. Il en résultera un gain en termes de coûts de construction, ainsi qu'un gain en termes de maintenance et de surveillance lors de l'exploitation. Enfin, les erreurs de maintenance (erreurs lors du remontage, oublis fermés, etc.) seront minimisées. Il en résultera un gain en termes de risque.

La robustesse de l'installation implique que la fonction de ses différents systèmes est toujours assurée, y compris lorsqu'ils sont utilisés hors de leur domaine de conception. Ainsi on peut, en développant la robustesse, se prémunir contre des imprévus, non considérés lors de la conception, qui apparaîtront lors de l'exploitation. On peut ainsi gagner en sûreté et en disponibilité.

Dans la section 3.2 du chapitre 1, on a vu que les lignes de défense devaient être indépendantes et concentriques [50]. Cet objectif rejoint les deux critères précédents. En effet, leur indépendance signifie que chacune d'elles doit être robuste en n'étant pas affectée par la défaillance des autres. La concentricité des lignes de défense, en contribuant à en réduire le nombre, simplifie l'installation.

La concentricité des lignes de défense s'obtient en les rendant les plus polyvalentes possible. Ainsi, chaque ligne de défense doit pouvoir arrêter ou diminuer la gravité de n'importe quelle séquence accidentelle, quel que soit l'état (pression, température, etc.) de la tranche.

L'indépendance des lignes de défense signifie que chaque ligne de défense peut remplir sa fonction quel que soit l'état des autres lignes de défense.

2.2.2 Mise en œuvre de ces objectifs qualitatifs

Contexte

En se fondant sur les principes énoncés dans la section précédente et en appliquant le critère de défaillance unique proposé dans la section 1, la centrale a été conçue à l'aide d'une approche déterministe haut niveau qui s'inspire de celle mise en œuvre lors de la conception des centrales actuelles. On crée ensuite l'EPS compacte.

Objectifs

Le premier objectif que nous poursuivons dans cette section est de s'assurer que le risque résiduel espéré peut être atteint avec le design envisagé et, le cas échéant, de redéfinir les lignes de défense pour pouvoir l'atteindre.

Le second objectif consiste à s'assurer que cette conception est robuste et en particulier que le critère de défaillance unique est bien décliné au niveau de chaque système.

Méthode

Vérifier la complétude : Avant de travailler à proprement parler avec le modèle compact, on doit s'assurer de sa complétude : il faut, avant de s'en servir comme outil d'aide à la décision, s'assurer qu'il couvre bien tous les cas possibles. Ainsi, l'élaboration des arbres d'événements doit être faite soigneusement. C'est l'exhaustivité de cette recherche des trajectoires accidentelles qui garantit que tous les risques ont été envisagés et qui assurera la bonne qualité de la conception faite à partir de ce modèle.

Dans la mesure où on est face à une EPS à la conception modélisant des systèmes pour lesquels on a peu ou pas de retours d'expérience, il peut être utile d'ajouter à la liste des arbres d'événements débutant par des initiateurs correspondant à des événements clairement identifiés, des arbres d'événements correspondant à des initiateurs que nous nommerons "flous". Ces initiateurs flous modélisent des événements qui peuvent avoir un impact fort sur la sûreté de l'installation, dont on ne connaît ni la cause ni le mode d'occurrence, mais dont l'impossibilité de l'occurrence ne peut pas être démontrée.

Ces initiateurs flous peuvent être définis lorsque l'on n'arrive pas à approfondir une analyse

causale du ou des événements redoutés jusqu'à un niveau de détail suffisant.

Exemple d'analyse causale : Pour illustrer ce que peut être une analyse causale, on peut prendre l'exemple de l'événement "rupture de la première barrière physique". Cette rupture peut avoir pour cause une fusion de cette barrière et/ou une rupture suite à un choc et/ou suite à un gonflement du combustible et/ou suite à un phénomène de fissuration et/ou de corrosion. Chacune de ces causes peut être détaillée. Ainsi, la rupture suite à un choc peut être divisée entre : choc avec un corps migrant, choc suite à une chute en fond de cuve, choc durant le rechargement du cœur, etc. Le niveau de détail à atteindre dépend de la diversité des parades à mettre en œuvre suivant les cas. Si quelles qu'en soient les causes, la rupture d'une gaine entraîne la mise en œuvre des mêmes parades, il ne sera pas utile de continuer la recherche des causes (excepté pour mieux pouvoir en définir la probabilité).

Pour tout événement dont on n'est pas capable de démontrer l'impossibilité de son occurrence mais dont on n'arrive pas à déterminer précisément les causes, on créera alors des initiateurs "flous". Si on peut affiner l'analyse causale de l'événement "rupture de la première barrière due à sa fusion" pour retrouver les initiateurs classiques des EPS de niveau I (brèches, pertes électriques, pertes du refroidissement, etc.), pour d'autres événements tels que "rupture d'une gaine de combustible suite à un choc avec un corps migrant", en revanche, on ne peut pas affiner l'analyse causale. On ne peut pas connaître la nature de ce corps ni sa provenance. On ne peut pas pour autant démontrer l'impossibilité d'un tel événement. On le considère donc comme un initiateur "flou".

Envisager l'occurrence d'initiateurs dont les causes ne sont pas bien définies contribue à la démonstration de sûreté. On se prémunit alors non seulement contre le prévu (les initiateurs clairement définis, les initiateurs déjà observés) mais aussi contre le possible (on ne sait pas bien pourquoi un événement peut se produire, mais on ne peut pas garantir qu'il ne se produise pas, donc on l'envisage).

Application du critère de défaillance unique : Dans un modèle compact où seuls les lignes de défense sont modélisées, vérifier le critère de défaillance unique revient à vérifier que la défaillance d'une seule ligne de défense n'entraîne pas l'occurrence de conséquences inacceptables et ce quel que soit l'initiateur considéré comme certain. Ce critère contribue à assurer la robustesse de l'installation car il revient à garantir son fonctionnement dans une multitude de modes dégradés.

Pour le vérifier, on génère les macro-coupes du modèle compact. Toutes les macro-coupes d'ordre égal ou inférieur à deux, c'est-à-dire toutes les macro-coupes ne contenant que l'occurrence d'un initiateur et de la défaillance d'au plus une ligne de défense, contreviennent à ce critère. Elles doivent être supprimées en modifiant la conception de la centrale. On pourra toutefois tolérer l'existence de macro-coupes ne contenant qu'une seule ligne de défense si la très faible probabilité d'occurrence de l'initiateur, ou la très bonne fiabilité de cette ligne de défense lorsque l'initiateur se produit, peuvent être démontrées.

Pour aider à la définition des modifications nécessaires à la suppression de ces macro-coupes d'ordre deux, nous proposons plusieurs types de regroupements. On peut regrouper ces coupes par initiateur ou famille d'initiateurs. On pourra alors établir si un type d'accident concentre la plupart des problèmes de non-respect du critère de défaillance unique. On peut dans ce cas choisir de modifier le domaine de couverture d'autres lignes de défense pour avoir une meilleure couverture du risque vis-à-vis de cet initiateur ou créer de nouvelles lignes de défense adaptées à ce contexte.

Pour ce faire, on identifie le ou les initiateurs (ou la famille d'initiateur) contenus dans des macro-coupes d'ordre un ou deux. Tous ces initiateurs appartiennent à des séquences accidentelles "trop courtes" au sens du critère de défaillance unique. On classe ensuite les initiateurs identifiés par ordre d'importance décroissant au moyen de l'indicateur de Butler (cf. page 37). En tête de classement apparaissent les initiateurs qui participent à beaucoup de macro-coupes d'ordre un ou deux.

Une fois identifiés les initiateurs posant problème, on doit modifier les lignes de défense associées à ces initiateurs. Pour chaque famille d'initiateurs posant problème, on identifie la ou les fonctions de sûreté reposant sur une seule ligne de défense (à partir des macro-coupes d'ordre deux). On peut alors créer une deuxième ligne de défense ou chercher, parmi les lignes de défense contribuant à la même fonction de sûreté, celles dont le domaine de couverture pourrait être étendu.

Exemple : Supposons qu'il existe, par exemple, une macro-coupe d'ordre deux : *Brèche* $\cap$ *Injection haute pression*. La fonction de sûreté consistant à refroidir le combustible n'est remplie que par une ligne de défense : l'injection haute pression. On peut alors envisager des modifications qui permettent à d'autres lignes de défense, comme *Injection moyenne pression*, de devenir redondantes avec l'injection haute pression lorsque l'initiateur *Brèche* se produit. On peut aussi créer une nouvelle ligne de défense en redondance avec l'injection haute pression.

Pour aider à la définition des modifications nécessaires à la suppression de ces macro-coupes d'ordre deux, on peut aussi les regrouper par lignes de défense. On pourra alors, le cas échéant, identifier la ou les lignes de défense dont la défaillance entraîne à elle seule la fusion dans de nombreux contextes. Il pourra être alors envisagé de créer une nouvelle ligne de défense fonctionnellement identique à cette ou ces lignes de défense qui posent problème.

Pour ce faire, on identifie les lignes de défense participant à des macro-coupes d'ordre deux. Toutes ces lignes de défense participent à des séquences accidentelles "trop courtes" au sens du critère de défaillance unique. On classe ensuite les lignes de défense identifiées par ordre d'importance décroissant au moyen de l'indicateur de Butler (cf. page 37). En tête de classement apparaissent les lignes de défense qui participent à beaucoup de macro-coupes d'ordre un ou deux.

Supposons que l'on ait identifié une ligne de défense i qui intervient dans des macro-coupes contrevenant au critère de défaillance unique. On peut alors chercher à identifier la ou les lignes de défense dont le domaine de couverture pourrait être étendu pour la ou les rendre redondantes avec la ligne de défense i. Pour aider à cette recherche, nous proposons d'établir, à partir de l'ensemble des macro-coupes, la liste des lignes de défense intervenant dans les mêmes macro-coupes que la ligne de défense i et contribuant à la même fonction de sûreté. On établit alors la liste des lignes de défense qui, dans d'autres contextes, sont redondantes avec la ligne de défense i. En effet, si une autre ligne de défense j est, dans certains contextes, fonctionnellement redondante avec la ligne de défense i, la défaillance simultanée de ces deux lignes de défense se retrouvera dans les macro-coupes correspondant à ces contextes. C'est dans cette liste que peuvent se trouver d'autres lignes de défense déjà en partie fonctionnellement redondantes avec i. Une fois ces lignes de défense identifiées, leur domaine de couverture pourra être étendu.

Enfin, si après ces deux types de regroupement, on n'arrive toujours pas à identifier clairement la nature du problème, on pourra regrouper par fonction de sûreté les lignes de défense dont la défaillance entraîne à elle seule la fusion. On pourra alors savoir quelle fonction de sûreté pose des problèmes en termes de défense en profondeur.

Exemple : Pour les centrales actuelles, on se rendra par exemple compte du fait que la fonction "contrôle de la réactivité" pose problème en termes de défense en profondeur. En effet, le non-fonctionnement de la ligne de défense "chute des grappes" entraîne à lui seul la fusion dans de nombreux arbres d'événements.

Après la modification de la conception à l'étude, le modèle EPS compact doit être mis à jour et on doit vérifier que, suite à ces modifications, le critère de défaillance unique est bien respecté, sauf éventuellement pour quelques lignes de défense très fiables associées à des initiateurs rares. Ces exceptions doivent être identifiées et justifiées.

Diminution du niveau de risque et du coût de construction et d'exploitation : Pour diminuer le risque, nous proposons de veiller à la concentricité des lignes de défense et à leur indépendance.

Concentricité
Cette concentricité contribue à la fois à la diminution du coût et à une bonne défense en profondeur. Pour la garantir, on doit s'assurer que chaque ligne de défense est la plus polyvalente possible, qu'elle remplit sa fonction quel que soit le contexte.

Pour s'assurer de la polyvalence des lignes de défense, on doit s'assurer que deux lignes de défense remplissant la même fonction sont bien fonctionnellement redondantes et non pas complémentaires (l'une ne fonctionnant que dans certains contextes et l'autre dans les autres). Pour ce faire, nous proposons de classer les lignes de défense selon leur fonction. Ce classement par fonction des lignes de défense est formalisé avec une liste de mots-clefs prédéfinis. Ainsi, chaque ligne de défense est caractérisée par un verbe décrivant son action, par exemple *refroidir*, par un complément d'objet direct décrivant à quoi s'applique cette action, par exemple *le circuit primaire*, et enfin par un ou plusieurs termes décrivant le contexte, par exemple *en situation incidentelle*. On obtient ainsi la classification de chaque ligne de défense selon sa fonction. L'ASG est alors décrite comme un système servant à *refroidir / le circuit primaire / en situation incidentelle*.

Une fois la description fonctionnelle de chaque ligne de défense faite, on vérifie que toutes les lignes de défense fonctionnellement voisines sont bien redondantes et non complémentaires. On se focalise donc sur les lignes de défense dont les deux premiers termes descriptifs sont identiques et qui ne sont pas redondantes. On évite ainsi que plusieurs systèmes remplissent la même fonction dans des contextes différents. Si c'est le cas, on peut, après avoir étendu le domaine de couverture de ces lignes de défense, soit obtenir des lignes de défense polyvalentes (fonctionnant quel que soit le contexte) et redondantes, soit en supprimer certaines pour diminuer le coût.

Exemple : Avec cette méthode, si on devait concevoir à nouveau les centrales existantes, on se rendrait compte que le RRA, l'ASG GCT atmo et l'ARE remplissent la même fonction dans des contextes différents : *refroidir / le circuit primaire / (en production / en situation incidentelle / à l'arrêt)*. On pourrait alors se poser la question d'étendre leur domaine de couverture pour qu'ils deviennent fonctionnellement redondants. On pourrait ainsi envisager des conditions de connexion au RRA moins strictes en termes de température et de pression, ou encore l'utilisation de l'ARE pour pallier à une défaillance de l'ASG en situation incidentelle.

La polyvalence de chaque ligne de défense est aussi déterminée en prenant en compte la multiplicité des contextes dans lesquels elle peut intervenir. Pour cela, nous proposons de rechercher les lignes de défense qui ne servent à se prémunir que contre un seul type d'initiateur ou contre un seul initiateur, ou encore dans une seule trajectoire accidentelle (c'est-à-dire dans une seule macro-coupe). Si on trouve des lignes de défense qui semblent n'intervenir que dans

un ou deux cas très précis, il faut étudier si une autre ligne de défense ne peut pas assurer cette fonction après avoir été légèrement modifiée. A l'inverse, on peut étudier l'intérêt d'utiliser cette ligne de défense trop pointue dans d'autres contextes pour accroître son utilité.

Suite à cette étude de la polyvalence des fonctions, des modifications de la conception de la centrale peuvent alors être décidées. Une fois ces modifications faites, le modèle compact doit être mis à jour et le critère de défaillance unique vérifié à nouveau.

Indépendance
Dans un second temps, il faut vérifier que tous les risques sont couverts. Pour cela, dans les macro-coupes courtes (d'ordre trois par exemple), la robustesse et l'indépendance des lignes de défense qui la composent seront vérifiées.

La vérification de l'indépendance fonctionnelle des lignes de défense d'une même macro-coupe est faite par un panel d'experts. Le but est ici d'identifier le ou les sous-systèmes dont la défaillance pourrait causer la perte de plusieurs lignes de défense d'une même macro-coupe. Ainsi, des experts ayant une bonne connaissance des systèmes qui peuvent correspondre à chaque ligne de défense devront estimer l'indépendance de chacune des lignes de défense de chaque macro-coupe courte. Par exemple, pour la macro-coupe : *perte réseau* ET *îlotage* ET *diesels*, des experts devront s'assurer qu'il n'existe pas, a priori, de défaillances de causes communes fonctionnelles entre ces trois événements (une alimentation électrique commune par exemple). Si on ne peut pas démontrer l'impossibilité de tels modes communs fonctionnels, on devra spécifier dans le cahier des charges que ces systèmes doivent être indépendants (des alimentations électriques séparées par exemple).

La vérification de la non-existence de modes communs externes doit aussi être réalisée. Dans ce cas, on ne recherche plus comme précédemment le ou les sous systèmes contribuant à plusieurs lignes de défense, mais la ou les causes externes non modélisées explicitement qui peuvent entraîner la perte de plusieurs lignes de défense d'une même macro-coupe. Cette vérification se fait en deux temps.

Dans un premier temps, on considère les macro-coupes courtes comme précédemment. Le but du panel d'experts est maintenant de chercher, pour chaque macro-coupe, la cause qui peut provoquer l'occurrence d'un mode commun entre toutes les lignes de défense et l'initiateur. Si on reprend l'exemple précédent, en supposant que la centrale considérée soit en bord de mer et que les diesels soient au niveau du sol, un ouragan peut provoquer la perte simultanée du réseau (la ligne s'est effondrée) et des diesels (noyés par des vagues passées au dessus des digues).

Dans un second temps, une démarche systématique est appliquée aux autres coupes. Pour ce faire, les causes externes pouvant affecter les lignes de défense doivent être listées. On peut par exemple identifier des causes telles que des températures élevées ou basses, une pression élevée, l'humidité, un incendie, des vibrations, la présence de rayonnements, des champs électromagnétiques, le vent, le terrorisme, etc. La robustesse de chaque ligne de défense à chacune de ces nuisances doit être définie comme : *RESISTE / NE RESISTE PAS / SANS OBJET*.

Par exemple, la résistance au vent des matériels situés dans le bâtiment réacteur est sans objet.

Enfin, chacune de ces nuisances est considérée comme certaine et on s'assure que dans chaque macro-coupe, au moins une ligne de défense résiste ou n'est pas soumise à la nuisance considérée comme certaine. Pour chaque nuisance, on crée ainsi un groupe PGT (cf. section 1.4 du chapitre 3) regroupant toutes les lignes de défense ne résistant pas à la nuisance étudiée. On regarde alors les modifications du jeu de macro-coupes de référence lorsque l'événement

$E_{1,PGT_{nuisance}}$ est certain[3] et on s'assure qu'aucune macro-coupe n'est réalisée.

Si ce n'est pas le cas, des modifications peuvent être envisagées en fonction de la vraisemblance de cette nuisance. De cette étude résulte aussi un cahier des charges qui spécifie, pour chaque ligne de défense, les nuisances auxquelles elle doit résister. Il est mis en œuvre lorsque le design de celle-ci est affiné.

Une fois les modifications de la conception de la centrale décidées, le modèle compact doit être mis à jour, le critère de défaillance unique revérifié, etc.

Suppression des lignes de défense inutiles ou peu utiles : Après toutes ces modifications et une fois le modèle EPS compact mis à jour, nous proposons de vérifier que toutes les lignes de défense sont utiles. En effet, on peut imaginer que certaines lignes de défense ne sont dans aucune macro-coupe minimale. Dans ce cas, cela veut dire que, d'après le modèle, leur bon fonctionnement ne permet jamais de diminuer la probabilité d'un accident. Une fois que ces lignes de défense présentes dans aucune coupe ont été identifiées et après accord des experts, on peut les supprimer. Le modèle compact sera alors mis à jour mais il ne sera pas utile de re-valider les étapes précédentes (critère de défaillance unique, polyvalence, etc.) car ces étapes sont basées sur les macro-coupes minimales.

On peut ensuite chercher à identifier les lignes de défense qui sont "peu" sollicitées. On pourra ainsi, pour chaque ligne de défense, isoler toutes les macro-coupes la contenant. Si elles sont toutes d'un ordre élevé, si les lignes de défense qui les composent sont bien fonctionnellement indépendantes et non sujettes aux même nuisances externes, et si elles sont peu nombreuses, on pourra envisager la suppression de la ligne de défense étudiée.

Pour aider à la mise en œuvre de cette démarche, nous proposons de classer toutes les lignes de défense suivant la classification de Butler. On ne considérera alors que les lignes de défense en fin de classement.

Si, après avis d'experts, on décide de supprimer des lignes de défense semblant peu utiles, il faudra mettre à jour le modèle compact et re-valider les étapes précédentes.

[3]Cet événement correspond à la défaillance simultanée de toutes les lignes de défense ne résistant pas à la nuisance considérée.

Schéma général de la méthode

La figure 4.2 résume les différentes étapes décrites dans la section 2.2. Elle illustre l'aspect itératif de la démarche que nous proposons.

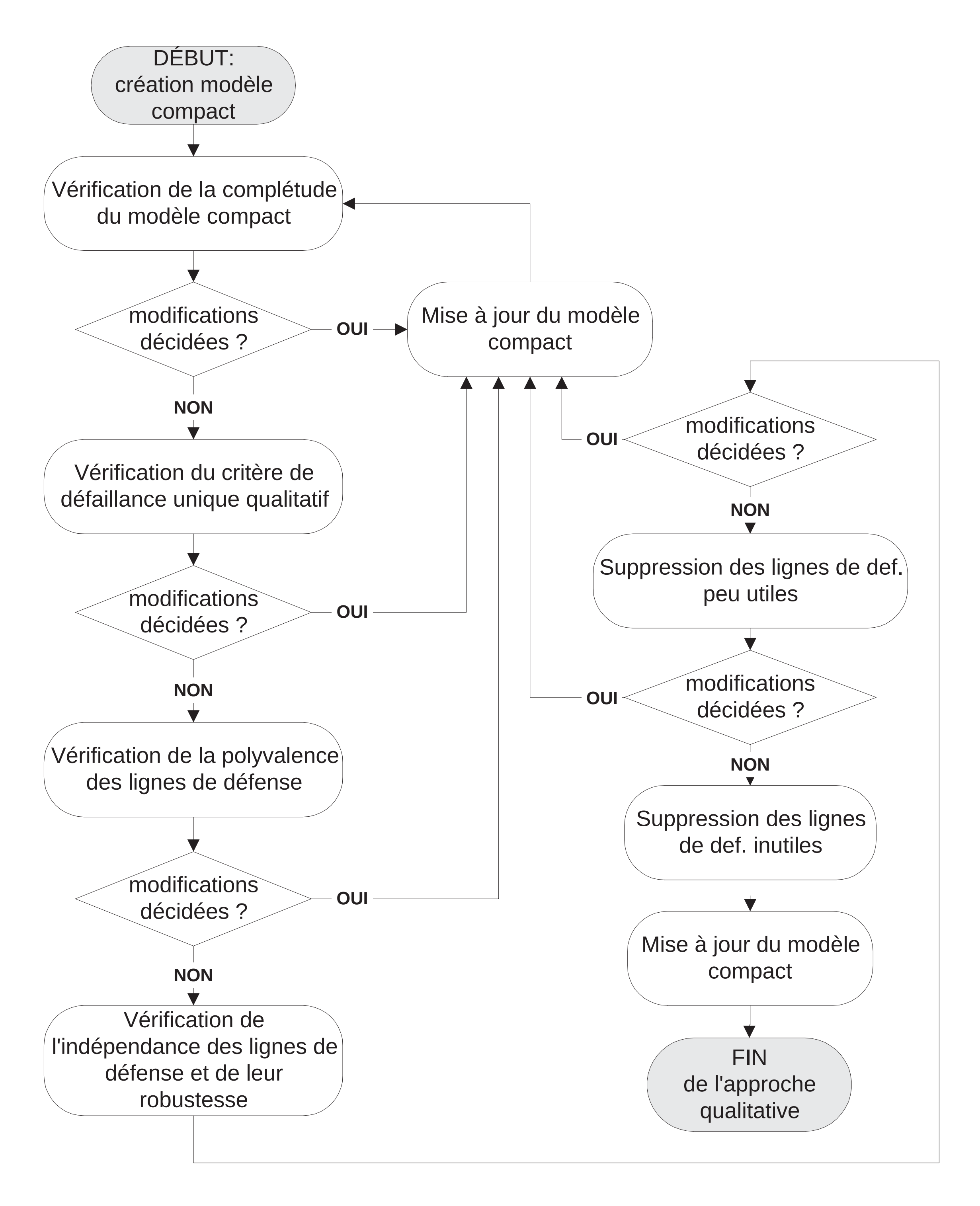


FIG. 4.2 – *Logigramme résumant les différentes étapes de l'utilisation qualitative du modèle compact*

2.3 Approche quantitative de la redéfinition des lignes de défense

Contexte

On dispose du modèle compact issu de l'étape précédente. On dispose d'une estimation grossière de la probabilité de défaillance de chaque ligne de défense (la probabilité qu'elle ne remplisse plus sa fonction) établie par avis d'expert. La probabilité d'occurrence des initiateurs flous auxquels on n'a pas pu attribuer de probabilité d'occurrence est mise à zéro (on ne considère plus les arbres d'événements qui y sont associés). Dans ce modèle compact, les événements "défaillance d'une ligne de défense i" sont considérés comme indépendants quel que soit i. Ceci est pris en compte en modélisant chaque ligne de défense au moyen d'un seul événement de base dans des logiciels qui considèrent les événements de base comme indépendants (c'est par exemple le cas de RSW).

On dispose alors d'une première estimation de la probabilité d'atteinte de conséquences inacceptables, qu'on nommera par la suite $R_{compact}$.

Objectif

L'objectif que nous poursuivons dans cette section est d'affiner la répartition des lignes de défense à partir d'une estimation probabiliste grossière de la probabilité d'occurrence des différentes macro-coupes et de vérifier de manière probabiliste le critère de défaillance unique appliqué au niveau des lignes de défense.

Méthode

Tout d'abord, on vérifie le niveau de défense en profondeur en appliquant le critère de défaillance unique probabiliste au niveau des lignes de défense. On comble ensuite les éventuelles lacunes en matière de protection contre les risques. Enfin, une fois qu'on arrive à un niveau de risque acceptable, on optimise le design en cherchant à augmenter la polyvalence de chaque ligne de défense et en supprimant les lignes de défense inutiles.

Vérification du critère de défaillance unique : Comme on l'a vu dans la section 1.3 de ce chapitre, la traduction littérale du critère de défaillance unique de manière probabiliste peut être formulée de la manière suivante :

L'accroissement de risque consécutif à la défaillance de n'importe quelle ligne de défense ne doit pas dépasser un certain seuil.

Pour obtenir la valeur de l'accroissement de risque, on peut calculer le FAR de chaque ligne de défense (d'autant plus facilement qu'elle est modélisée au moyen d'un événement de base et que son FAR est donc calculé de manière automatique dans Risk Spectrum) et le multiplier par $R_{compact}$ pour obtenir cet accroissement de risque. En effet, le numérateur du FAR d'une ligne de défense i ($= FAR\,(LD_i) \cdot R_{compact}$) nous donne l'accroissement de risque consécutif à l'occurrence de sa défaillance. Pour mémoire le FAR d'une ligne de défense s'exprime comme :

$$FAR\,(LD_i) = \frac{\overbrace{P\,(CI/LD_i)}^{R_{1,LD_i;compact}} - \overbrace{P\,(CI)}^{R_{compact}}}{P\,(CI)}$$

Si une ligne de défense ne vérifie pas ce critère de défaillance unique probabiliste (c'est-à-dire si l'accroissement de risque est supérieur au seuil), une modification de la centrale doit être envisagée car on est mal protégé contre la défaillance de cette ligne de défense.

Pour aider à l'identification des modifications nécessaires pour que la ligne de défense i vérifie le critère de défaillance unique, on peut regarder si les macro-coupes contenant la ligne de défense i et devenant prédominantes lorsque LD_i est réalisé ne peuvent pas être associées à un type de séquence, à un arbre d'événements ou à une famille d'initiateurs.

Si au moyen de ces regroupements, on peut n'identifier que quelques macro-coupes qui contribuent le plus fortement à l'accroissement de risque quand la défaillance de i est certaine,

alors on ne modifie dans un premier temps que les macro-coupes où i joue un rôle trop important. On peut, au cas par cas, y ajouter des lignes de défense nouvelles ou renforcer les lignes de défense autres que la ligne de défense i pour les rendre plus fiables.

Si ce n'est pas le cas, c'est-à-dire si de nombreuses macro-coupes correspondant à des contextes différents contribuent à cette valeur élevée de l'accroissement de risque lorsque LD_i est réalisé, on appliquera alors une solution générique qui consiste à créer une ligne de défense ayant la même fonction que i mais basée sur une technologie différente pour éviter les DCC entre systèmes. On créera alors une ligne de défense en redondance fonctionnelle avec i.

Vérification de la polyvalence des lignes de défense : La plus grande part de la réflexion sur la polyvalence des lignes de défense est menée lors de l'utilisation qualitative du modèle compact au moyen d'une analyse fonctionnelle. Toutefois, même si nous avons veillé, de manière qualitative, à ce que chaque ligne de défense intervienne dans de nombreuses trajectoires accidentelles, nous proposons d'enrichir cette analyse par une approche quantitative qui permet d'identifier les lignes de défense très voire trop pointues, c'est-à-dire insuffisamment polyvalentes pour justifier leur coût. En effet, une ligne de défense peut être présente dans de nombreux contextes mais ne contribuer à la diminution du risque ou à une bonne défense en profondeur que dans très peu de cas.

Pour identifier les lignes de défense qui sont trop pointues, on recherche les contextes dans lesquels les lignes de défense sont utiles. Pour ce faire, on calcule l'indicateur de Birnbaum de la ligne de défense étudiée au sein de chaque arbre d'événements. Cet indicateur, sous l'hypothèse que le fonctionnement de la centrale soit cohérent, traduit la probabilité que la ligne de défense étudiée soit critique. Il renseigne donc sur le fait que cette ligne de défense soit utile dans la mesure où il donne la probabilité qu'elle soit indispensable. Si l'indicateur de Birnbaum de la ligne de défense n'est non négligeable que du fait d'un seul arbre ou de quelques arbres de la même famille, on regarde au sein de ces arbres dans quels types de séquence cette ligne de défense intervient. Enfin, on étudie la possibilité de faire remplir la fonction de cette ligne de défense par une autre ligne de défense dont on étendrait le domaine de couverture. Pour identifier la ligne de défense qui pourrait permettre cette substitution, on peut s'inspirer de la démarche proposée dans le cadre de l'approche qualitative. Le cas échéant, si cette substitution est possible et se traduit par une réduction de coût, on étudiera, avant de décider cette modification, l'impact de la suppression de la ligne de défense étudiée sur le niveau de défense en profondeur.

Réduction de la valeur du risque de référence : Si le risque de référence estimé avec le modèle compact ($R_{compact}$) est supérieur au risque résiduel souhaité, il faut modifier la conception de la centrale pour le diminuer. Pour ce faire, on travaille tout d'abord sur les quelques macro-coupes les plus probables qui, à elles seules, constituent la plus grande part du risque. Ensuite, si c'est encore nécessaire, on peut chercher à identifier les lignes de défense qui contribuent le plus au risque pour les renforcer, ou chercher les types d'accidents qui contribuent le plus au risque pour rajouter des lignes de défense permettant d'en diminuer l'importance.

Dans un premier temps, nous proposons donc de modifier les quelques macro-coupes dominantes qui contribuent fortement à la valeur de $R_{compact}$. Lorsque ces macro-coupes dominantes sont identifiées, on peut améliorer la fiabilité des lignes de défense qui les composent ou les compléter par d'autres lignes de défense.

Une fois ces modifications faites, le modèle compact remis à jour et le critère de défaillance unique probabiliste re-vérifié, on calcule à nouveau $R_{compact}$. Si cette valeur est toujours supérieure au risque résiduel souhaité, il faut encore diminuer ce risque. Le problème est alors qu'il n'y a plus forcément de macro-coupes dominantes. En effet, ces macro-coupes ont été modifiées pour diminuer leur probabilité d'occurrence. On se retrouve alors face à un grand nombre de

macro-coupes plus ou moins équiprobables et il devient difficile de savoir par quel biais diminuer encore le risque. Dans ce cas, deux approches sont possibles : soit on identifie les lignes de défense qui contribuent fortement au risque pour les renforcer ou les redonder, soit on cherche à déterminer quels arbres d'événements, quels types de séquences, composent la plus grande part du risque pour créer de nouvelles lignes de défense les plus utiles possible.

Pour identifier les types d'accidents qui pèsent le plus sur le risque, on peut calculer le FDR d'un initiateur, d'une famille d'initiateurs (au moyen d'un groupe PGT contenant l'ensemble des initiateurs de la famille) ou encore d'une famille de fonctions (un groupe PGT englobant les lignes de défense dont la fonction appartient à la famille). En effet, le FDR d'un événement renseigne sur sa contribution au risque. On sera alors en mesure de voir plus précisément où se trouvent les lacunes de la conception à l'étude et de les combler.

Si on ne veut pas rechercher de nouvelles fonctions utiles à la diminution du risque et ainsi remettre significativement en cause la conception à l'étude, on peut aussi diminuer le risque en améliorant les lignes de défense existantes. Pour ce faire, nous proposons de calculer le FDR et l'indicateur de Birnbaum (IB) de chaque ligne de défense. On s'inspire alors des types de classification de la démarche OMF présentée dans la section 3.1 du chapitre 1. Les différences notables avec cette approche sont qu'on ne considère plus des événements élémentaires mais des événements associés à des lignes de défense et que l'emploi du FAR est remplacé par celui de l'indicateur de Birnbaum. On a alors la classification suivante :

- Si l'IB d'une ligne de défense est élevé sans que son FDR le soit, alors cette ligne de défense joue un rôle important et le remplit efficacement. Aucune modification ne doit être envisagée.
- Si l'IB d'une ligne de défense est élevé et si son FDR l'est aussi, la ligne de défense étudiée joue un rôle important dans la prévention des accidents mais ne le remplit qu'imparfaitement. Deux types d'actions sont possibles. Soit on est capable d'identifier dans quelle(s) trajectoires(s) accidentelle(s) cette ligne de défense est très utile et trop perméable, et dans ce cas, on peut travailler au développement ou à l'extension d'une ligne de défense dans ce contexte spécifique. Soit la ligne de défense étudiée a un FDR élevé car elle intervient dans de nombreux contextes et dans ce cas, il serait plus avantageux de redonder cette ligne de défense par une autre fonctionnellement identique mais techniquement différente pour éviter les modes communs, ou encore de chercher à améliorer la fiabilité de la ligne de défense à l'étude.
- Si le FDR d'une ligne de défense est relativement élevé sans que son IB le soit, alors elle joue un rôle limité et le remplit mal. L'opportunité d'améliorer cette ligne de défense doit être envisagée en fonction du coût de cette amélioration.
- Si le FDR et l'IB d'une ligne de défense sont faibles, la suppression de cette ligne de défense peut être envisagée. La méthode pour supprimer les lignes de défense inutile sera développée dans la partie qui suit.

Le cas échéant, on décide alors de procéder à des modifications. Une fois qu'elles ont été définies, le modèle compact doit être remis à jour et le processus de validation repris depuis son commencement.

En résumé, le risque de référence est diminué en modifiant les coupes dominantes puis, une fois qu'il n'y a plus de coupes dominantes, en créant de nouvelles lignes de défense les plus utiles possible et/ou en renforçant les lignes de défense existantes qui en ont le plus besoin.

Suppression des lignes de défense inutiles : Normalement, durant la phase qualitative de la répartition des lignes de défense, les lignes de défense qui ont été conçues lors de la démarche déterministe et qui n'apparaissent dans aucune macro-coupe ont été éliminées. Il reste donc à supprimer les lignes de défense qui semblaient être utiles lors d'une approche

structurelle et qui s'avèrent inutiles une fois qu'on considère la valeur du risque. Pour ce faire, on calcule l'indicateur de Birnbaum de chaque ligne de défense. Si la valeur de cet indicateur est très faible, cela signifie que la ligne de défense étudiée est très rarement sollicitée et donc potentiellement inutile. Toutefois, certaines lignes de défense paraissant inutiles peuvent être nécessaires au respect du critère de défaillance unique.

Exemple : Si on suppose l'existence d'un initiateur "perte de la turbine" dont l'occurrence nécessite l'arrêt du réacteur qui est obtenu par la chute des "barres de contrôle", l'application du critère de défaillance unique conduira à créer un autre système d'arrêt du réacteur, par exemple "chute des barres d'arrêt d'urgence (A.U.)". En effet, sans ce second système et en supposant que le non-arrêt du cœur conduise aux conséquences inacceptables, on aurait une macro-coupe d'ordre deux : *perte turb.* ET *barres contrôle*, qu'on ne peut pas accepter. On crée donc un deuxième système fonctionnellement identique pour obtenir la macro-coupe : *perte turb.* ET *barres contrôle* ET *barres A.U.* . Supposons maintenant que la ligne de défense "barres de contrôle" soit très fiable. Alors la ligne de défense "barres A.U." est très rarement sollicitée, donc très rarement critique. Pourtant, cette ligne de défense n'est pas inutile car elle garantit un bon niveau de défense en profondeur relativement à l'événement "non-chute des barres de contrôle".

Pour identifier les lignes de défense qui ne sont utiles ni pour le risque ni pour la défense en profondeur, nous proposons la démarche suivante. Une ligne de défense i sera jugée inutile et sera supprimée si elle vérifie l'ensemble des conditions suivantes :

1. L'indicateur de Birnbaum de l'événement "indisponibilité de la ligne de défense i" (E_{LD_i}) est très faible.
2. Le FARP de toutes les autres lignes de défense, lorsqu'on considère que i est indisponible, reste acceptable. C'est à dire que :

   $$FARP\left(E_{LD_j}/E_{LD_i}\right) < seuil \quad \forall E_{LD_j}$$

   Si c'est le cas, le critère de défaillance unique probabiliste sera toujours respecté une fois la ligne de défense i supprimée.
3. La suppression de la ligne de défense i ne produit pas de macro-coupe d'ordre deux. Si c'est le cas, on respecte bien le critère de défaillance unique qualitatif. Dans cette étape, il faudra aussi considérer les arbres d'événements contenant des initiateurs flous. En effet, ce n'est pas parce qu'on ne peut pas quantifier la probabilité d'occurrence de ces initiateurs qu'ils ne doivent pas être considérés dans la défense en profondeur.
4. Cette ligne de défense ne contribue pas à éviter des événements qui ne sont pas modélisés dans les EPS, tels que le confinement des matières radioactives ou la protection des systèmes permettant le redémarrage de l'installation.
5. Le panel d'experts consulté est favorable à sa suppression.
6. Son coût de construction ou d'exploitation n'est pas négligeable.

Toute suppression d'une ligne de défense doit conduire à une mise à jour immédiate du modèle compact avant d'envisager une autre suppression. En effet, un modèle à jour est nécessaire à la vérification des critères de défaillance unique probabiliste et qualitatif.

Dans la mesure où seules les lignes de défense inutiles ont été supprimées, l'étape quantitative du processus de répartition des lignes de défense (vérification de la polyvalence et réduction du risque) ne doit pas être repris à son début comme pour les autres étapes de cette démarche.

Schéma global de la démarche

La figure 4.3 résume les différentes étapes de la section 2.3 de ce chapitre.

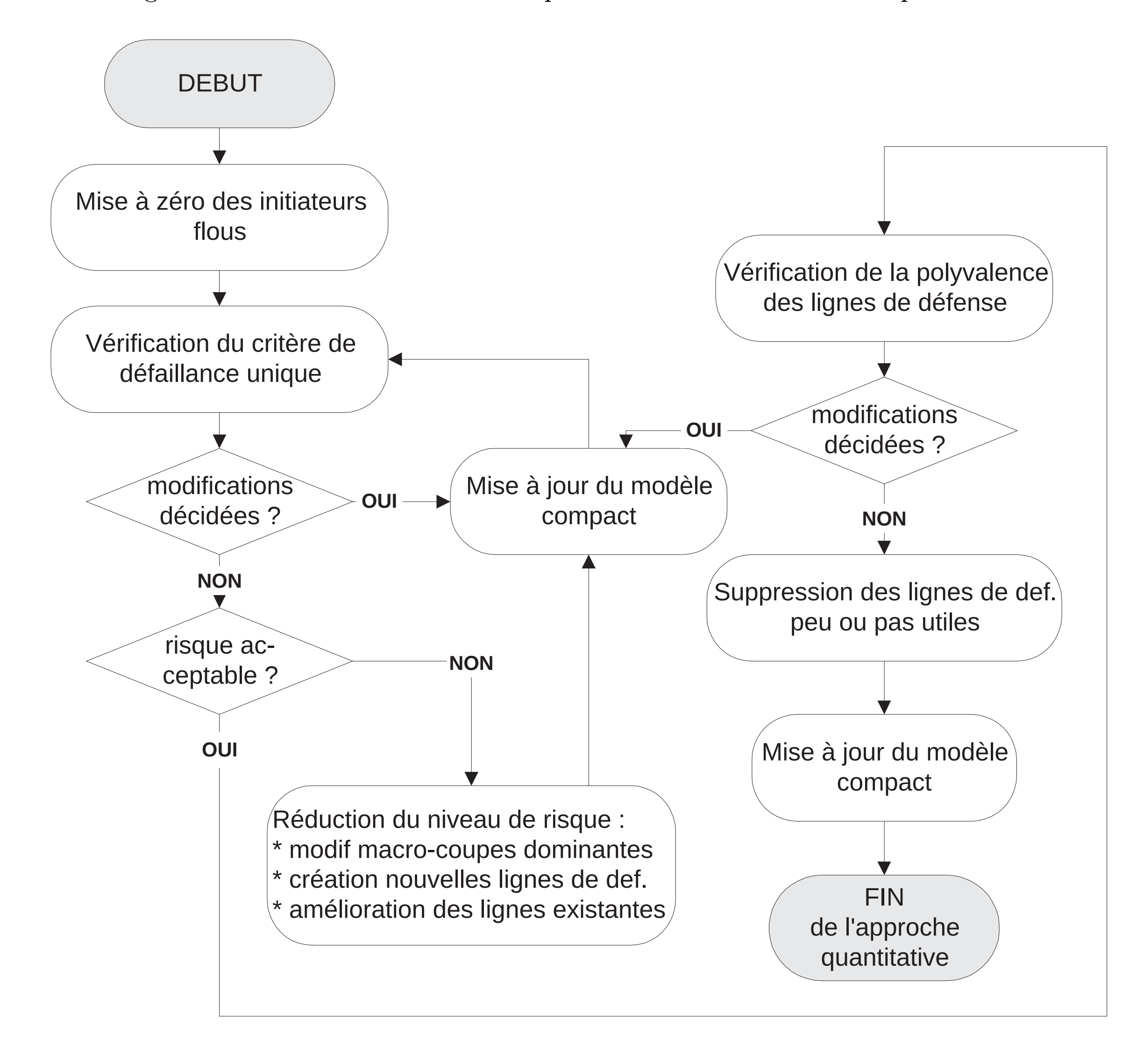


FIG. 4.3 – *Schéma résumant les différentes étapes de l'utilisation quantitative du modèle compact*

3 S'assurer de l'indépendance des lignes de défense

Contexte

Durant la seconde étape de notre processus de conception, à l'aide du modèle EPS compact, de nouvelles lignes de défense ont été créées, d'autres ont été modifiées ou supprimées pour aboutir à une conception qui maximise la sûreté de la centrale à l'étude. Néanmoins, suite à cette première utilisation d'une approche probabiliste, on ne dispose que de la conception "fonctionnelle" de la centrale (on ne sait pas comment chaque ligne de défense remplit sa fonction). La troisième étape de notre démarche de conception permet alors de concevoir les systèmes remplissant la fonction de chaque ligne de défense au moyen d'une démarche déterministe conventionnelle. On dispose ainsi d'un plan détaillé allant jusqu'au niveau composant de la centrale à l'étude. On peut alors créer un modèle EPS complet (par opposition avec le modèle compact) qui modélise l'ensemble des composants contribuant aux différentes lignes de défense et aux différents initiateurs. Dans ce modèle complet, chaque ligne de défense n'est plus modélisée par un simple événement de base, mais par un arbre de défaillances modélisant l'échec de la fonction de la ligne de défense à partir de chacun de ses composants. Avec le modèle complet, on peut exprimer le risque en termes de macro-coupes mais aussi en termes de coupes minimales de référence. Une macro-coupe sera l'intersection de macro-événements, alors qu'une coupe de référence sera l'intersection d'événements élémentaires. Chaque coupe de référence peut appartenir à une ou plusieurs macro-coupes. C'est le cas de la coupe $EB_{Init} \cap EB_2$ de la figure 4.1 page 115, qui appartient à la fois à la macro-coupe $Initiateur \cap LD_2$ et $Initiateur \cap LD_1$.

Ce modèle complet est aussi utilisé pour remettre à jour le modèle compact. Ainsi, la probabilité de défaillance de chaque ligne de défense est obtenue grâce aux arbres de défaillances du modèle complet modélisant ces défaillances. Les probabilités ainsi calculées sont alors réinjectées dans le modèle compact pour remettre à jour la probabilité d'occurrence des EB_{LD_i}. De même, si de nouveaux arbres d'événements ont été créés lors de l'élaboration du modèle complet, ces arbres sont ajoutés dans le modèle compact. En résumé, la seule différence entre modèle compact et modèle complet réside dans le fait que dans le modèle compact, toutes les lignes de défense et tous les initiateurs sont considérés comme indépendants et modélisés au moyen d'un unique événement de base.

Les arbres d'événements débutant par l'occurrence d'un initiateur "flou" sont aussi présents dans le modèle complet. Pour pouvoir les prendre en compte dans l'EPS complète, on doit essayer de définir, au moyen d'avis d'experts, la probabilité d'occurrence de ces événements initiateurs "flous". S'il n'est pas possible, même de manière très conservative, de définir une probabilité d'occurrence pour certains de ces événements initiateurs, on les néglige en leur attribuant une probabilité d'occurrence nulle. Ainsi, les arbres d'événements qui y sont associés sont présents dans le modèle mais ils ne sont pas pris en compte lorsque le risque est calculé.

Cette démarche s'inspire de l'approche que nous avons proposée dans [33]

Objectif

Dans la section 2 de ce chapitre, les lignes de défense ont été conçues pour garantir une répartition homogène des moyens et une atteinte à moindre coût du niveau de risque résiduel voulu. Cependant, cette répartition a été faite en négligeant les interdépendances entre lignes de défense. Lors de la conception des systèmes remplissant la fonction de chaque ligne de défense, il faudra donc s'assurer qu'il n'existe pas, entre les lignes de défense, de causes communes fonctionnelles pénalisantes pour le risque ou la sûreté. En effet, si plusieurs lignes de défense situées sur la même trajectoire accidentelle (dans la même macro-coupe) partagent un ou plusieurs même(s) sous-système(s), la défaillance de ce(s) sous-système(s) entraînera la défaillance, ou du moins l'affaiblissement simultané, de ces lignes de défense et donc un accroissement important de la probabilité d'accident. D'après Frank [51], ces interdépendances entre ligne de

défense constituent "*des contributrices majeures à la valeur du risque de référence*" dans les centrales actuelles. Ces interdépendances ne peuvent pas être identifiées avec le modèle compact car les sous-systèmes n'y sont pas modélisés. Chaque ligne de défense y est considérée comme indépendante des autres.

Méthode

Les différentes lignes de défense de la centrale à l'étude peuvent être interdépendantes car elles partagent des sous-systèmes ou des composants. D'un certain point de vue, ces interdépendances sont utiles car elles contribuent à diminuer le coût global de la centrale à l'étude en diminuant le nombre de sous-systèmes remplissant la même sous-fonction. D'un autre côté, ces modes communs fonctionnels rendent interdépendantes les différentes lignes de défense partageant un ou plusieurs sous-systèmes. Elles sont alors sujettes à des défaillances de causes communes fonctionnelles liées à ces sous-systèmes. L'existence de ces causes communes peut entraîner une augmentation du risque ou un affaiblissement du niveau de défense en profondeur si elles affectent plusieurs lignes de défense ou initiateurs appartenant à la même trajectoire accidentelle, c'est-à-dire à une même macro-coupe. Ainsi, pour minimiser le risque et maximiser l'utilisation des sous-systèmes, seules les lignes de défense appartenant à une même macro-coupe doivent être indépendantes. Toutes les lignes de défense qui ne sont jamais dans les mêmes macro-coupes peuvent être très interdépendantes. La figure 4.4 illustre le fait que seules les interdépendances entre lignes de défense appartenant à une même macro-coupe ont un impact sur le risque. Cette figure nous présente deux macro-coupes : $(Initiateur \cap LD_1 \cap LD_{2.1} \cap LD_3)$ et $(Initiateur \cap LD_1 \cap LD_{2.2} \cap LD_3)$. Lorsque la ligne de défense 2.1 est défaillante, le fonctionnement ou la panne de la ligne de défense 2.2 ne sont plus importants. Même si les lignes de défense 2.1 et 2.2 sont très interdépendantes, ces interdépendances ne contribuent pas à augmenter le risque. En effet, si l'une des deux est défaillante, l'autre est "court-circuitée" et son état (marche ou panne) n'a plus d'importance. Par contre, les lignes de défense 1, 2.1 et 3 doivent être indépendantes pour garantir qu'elles ne soient pas défaillantes en même temps (de même que les lignes de défense 1, 2.2 et 3).

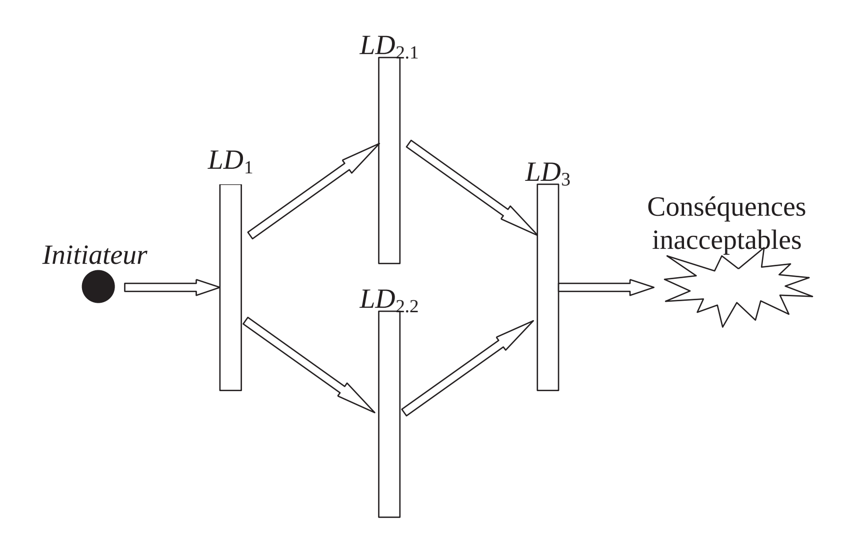


FIG. 4.4 – *Exemple de répartition des lignes de défense*

Notre démarche de réduction des modes communs fonctionnels est donc principalement centrée sur l'étude des macro-coupes. Elle se déroule en plusieurs temps. Tout d'abord, on identifie et on supprime les interdépendances entre lignes de défense qui pèsent sur le risque. Pour supprimer ces interdépendances, on diversifie les matériels ou les sous-systèmes partagés

par plusieurs lignes de défense d'une même macro-coupe. C'est à dire qu'on crée un sous-système spécifique pour chaque ligne de défense. Ensuite, on vérifie que des interdépendances de très faible probabilité qui ne pèsent pas sur le risque ne peuvent pas provoquer un énorme accroissement de risque lorsque qu'une cause commune fonctionnelle survient. Puis on étudie l'impact des modes communs fonctionnels sur la défense en profondeur davantage que leur contribution au risque. On vérifie le respect du critère de défaillance unique au niveau des composants. Enfin, les matériels et lignes de défense rendus inutiles par les interdépendances sont supprimés.

3.1 Résumé de la démarche

Pour identifier les interdépendances fonctionnelles, en estimer l'importance et les réduire, on emploie une démarche itérative. Elle se déroule en quatre temps : réduire les interdépendances entre lignes de défense significatives pour le risque, puis réduire les interdépendances significatives pour la sûreté (affaiblissant le niveau de défense en profondeur), puis vérifier le critère de défaillance unique au niveau des matériels et enfin, supprimer les matériels et lignes de défense qui s'avèrent inutiles.

Cette démarche s'inspire de la démarche que nous avons proposée dans [33].

Interdépendances significatives pour le risque : La première étape de la démarche, c'est-à-dire la réduction des interdépendances significatives pour le risque, est menée à bien de la manière suivante :

- l'impact global des interdépendances est estimé,
- les trajectoires accidentelles contenant les interdépendances qui pèsent sur le risque sont identifiées,
- les composants qui causent ces interdépendances sont identifiés,
- parmi les sources d'interdépendances identifiées, celles qui peuvent être supprimées le sont.

Au terme de ce processus, le modèle EPS complet est mis à jour et l'impact des interdépendances sur le risque est à nouveau estimé. S'il est devenu acceptable, on passe à l'étape suivante ; sinon, on reprend ces quatre étapes à leur début.

Défense en profondeur et interdépendances significatives pour la sûreté : La deuxième étape de la démarche vise à s'assurer de manière quantitative du bon niveau de défense en profondeur en appliquant le critère de défaillance unique probabiliste au niveau des EB. Pour les identifier, on détermine les événements de base dont l'occurrence certaine engendre un accroissement de risque non acceptable. On identifie alors les EB qui sont intrinsèquement importants pour la sûreté et ceux qui sont importants parce que leur occurrence affaiblit plusieurs lignes de défense d'une même macro-coupe. Les matériels qui correspondent à des EB qui sont intrinsèquement importants pour la sûreté doivent être redondés. Les matériels qui génèrent des modes communs au sein des lignes de défense d'une même macro-coupe doivent être diversifiés. C'est à dire que chaque ligne de défense doit avoir son matériel spécifique. En effet, ces matériels peuvent ne participer qu'à un petit nombre de lignes de défense, mais si celles-ci sont successives, la défaillance de ces matériels augmente significativement la probabilité d'occurrence de la macro-coupe. Pour identifier les EB correspondant à des interdépendances significatives pour la sûreté au sein d'une même macro-coupe, on applique, pour chaque EB significatif pour la sûreté, la démarche suivante :

- Les macro-coupes où cet EB est significatif pour la sûreté sont identifiées.
- Dans chacune des macro-coupes identifiées, on regarde si cet EB est important pour plus d'une ligne de défense.

Si c'est le cas, alors cet EB correspond, dans cette macro-coupe, à des interdépendances entre ses lignes de défense significatives pour la sûreté. Le matériel correspondant à cet EB doit être diversifié. Si ce n'est pas le cas, c'est-à-dire si un EB dont l'occurrence certaine engendre un accroissement de risque non-acceptable ne génère aucune interdépendance significative pour la sûreté au sein d'une même macro-coupe, alors il est intrinsèquement important pour la sûreté. Il doit donc être redondé.

Une fois cette modification de la conception à l'étude effectuée, on pourra vérifier à nouveau s'il n'est pas aussi intrinsèquement important pour la sûreté.

Critère de défaillance unique qualitatif : On vérifie que le critère de défaillance unique qualitatif est bien vérifié au niveau des événements de base. C'est à dire qu'on vérifie qu'il n'existe pas de coupes d'ordre un ou deux. Le cas échéant, on justifie le caractère acceptable de telles coupes ou on modifie la conception à l'étude pour les supprimer.

Critère de validation de ces étapes : Au terme de ce processus, le modèle EPS complet est mis à jour et l'impact des interdépendances sur la sûreté est à nouveau estimé. S'il est devenu acceptable et que les deux critères de défaillance unique (qualitatif et quantitatif) sont validés, on passe à l'étape suivante. Sinon, on reprend ces trois étapes à leur début.

Composants et lignes de défense inutiles : Du fait des interdépendances acceptées dans les deux étapes précédentes, certains composants et certaines lignes de défense peuvent s'avérer inutiles. Dans ce cas, sauf avis d'expert contraire, on les supprime.

3.2 Estimation de l'impact global des interdépendances entre lignes de défense

Pour estimer l'impact global des interdépendances sur le risque, on compare le risque estimé par le modèle compact à celui estimé par le modèle complet. En effet, la seule différence entre ces deux modèles réside dans le fait que le premier néglige les interdépendances entre lignes de défense liées aux sous-systèmes et composants partagés, à l'inverse du second. Cela est dû au fait que chaque ligne de défense est modélisée, dans le modèle compact, au moyen d'un simple événement de base considéré comme indépendant des autres. On obtient ainsi $\Delta_{R,DF}$, qui est l'écart de risque lié aux dépendances fonctionnelles.

$$\Delta_{R,DF} = R_{complet} - R_{compact}$$

Cet écart est le plus souvent positif, les interdépendances contribuant à augmenter le risque. Cependant il peut aussi, du moins en théorie, être négatif s'il y a des interdépendances entre des lignes de défense qui ne sont pas sur les même trajectoires accidentelles. Si on reprend l'exemple de la figure 4.1 page 115, on voit que le risque correspond à $P\left(Initiateur \cap LD1 \cup Init \cap LD2\right)$. Le modèle compact calculera $R_{compact}$ comme :

$$\begin{aligned}
R_{compact} &= P\left(EB_{Init} \cap EB_{LD1} \cup EB_{Init} \cap EB_{LD2}\right) \\
&\underset{\substack{approximation\\ événements\\ rares}}{\approx} \overbrace{P\left(Init_1\right)}^{P(EB_{Init})} \cdot \overbrace{\left(P\left(EB_1\right) + P\left(EB_2\right) + P\left(EB_3\right) \cdot P\left(EB_4\right)\right)}^{P\left(EB_{LD_1}\right)} \\
&\qquad + \underbrace{P\left(Init_1\right)}_{P(EB_{Init})} \cdot \underbrace{\left(P\left(EB_2\right) + P\left(EB_3\right)\right)}_{P\left(EB_{LD_2}\right)} \\
&\underset{\substack{approximation\\ événements\\ rares}}{\approx} P\left(Init_1\right) \cdot \left[P\left(EB_1\right) + 2 \cdot P\left(EB_2\right) + P\left(EB_3\right) \cdot \left(1 + P\left(EB_4\right)\right)\right]
\end{aligned}$$

alors que la vraie probabilité $R_{complet}$ est de :

$$\begin{aligned} R_{complet} &= P\left(Initiateur \cap LD1 \cup Initiateur \cap LD2\right) \\ &= P\left(Init_1 \cap EB_1 \cup Init_1 \cap EB_2 \cup Init_1 \cap EB_3\right) \\ R_{complet} &\underset{\substack{approximation \\ \text{événements} \\ rares}}{\approx} P\left(Init_1\right) \cdot \left[P\left(EB_1\right) + P\left(EB_2\right) + P\left(EB_3\right)\right] \end{aligned}$$

La probabilité $P\left(EB_{LD_i}\right)$ est calculée à partir de l'arbre de défaillances du modèle complet modélisant le macro-événement LD_i.

On a donc $R_{compact} > R_{complet}$ et donc $\Delta_{R,DF} < 0$, car EB_2 crée des interdépendances entre macro-coupes, ce qui contribue à diminuer le risque. En effet, avec le modèle complet, on ne compte pas deux fois la coupe minimale $EB_{init} \cap EB_2$, ce qui est en revanche le cas dans le modèle compact. De plus, dans le modèle compact, on prend en compte la probabilité associée à la coupe $EB_3 \cap EB_4$ qui est non-minimale et donc supprimée du jeu de coupes dans le modèle complet (car il existe la coupe $Init \cap EB_3$, qui est plus courte).

On dispose maintenant d'une estimation ($\Delta_{R,DF}$) de l'impact des interdépendances sur le risque. Il reste à voir s'il est acceptable et, le cas échéant, comment on peut le minimiser.

3.3 Interdépendances significatives pour le risque

Objectif

Le but de la démarche que nous proposons dans cette partie est de réduire le surcroît de risque lié aux interdépendances entre lignes de défense appartenant aux mêmes macro-coupes, de manière à atteindre la valeur de risque choisie lors de la conception des lignes de défense, c'est-à-dire la valeur de $R_{compact}$ obtenue après les étapes qualitatives et quantitatives d'enrichissement de la conception.

Si $\Delta_{R,DF}$ est négatif ou presque nul, cette valeur est déjà atteinte, il n'y a donc pas besoin de réduire les interdépendances significatives pour le risque. Le développement ci-dessous est alors sans objet.

Méthode

La démarche qui vise à l'identification et au traitement des interdépendances pénalisantes pour le risque se décompose en plusieurs étapes. Tout d'abord, les arbres d'événements contenant ces interdépendances pénalisantes sont identifiés. Ensuite, on identifie parmi les macro-coupes de ces arbres celles qui contiennent des interdépendances significatives pour le risque. On détermine alors les lignes de défense de ces macro-coupes qui sont liées par des modes communs. On identifie aussi leurs composants partagés et les coupes minimales associées à ces macro-coupes qui contiennent le plus d'interdépendances. Enfin, des modifications sont décidées pour réduire ces interdépendances là où c'est possible.

Identification des arbres d'événements contenant des interdépendances significatives pour le risque : Pour identifier ces arbres, on compare le risque associé à chaque arbre d'événements lorsqu'il est estimé avec le modèle compact et avec le modèle complet. C'est à dire que l'on calcule $\Delta_{R,DF}|_{A.E._i}$ uniquement pour l'arbre d'événements i (noté $A.E._i$). Cela revient à comparer la probabilité de l'union des macro-coupes du modèle compact qui sont issues de cet arbre d'événements i avec la probabilité de l'union des coupes de référence du modèle complet qui sont issues de ce même arbre d'événements i. Si un arbre d'événements contribue pour plus d'un certain pourcentage ($\Delta_{R,DF}|_{A.E._i}/\Delta_{R,DF}$>5% par exemple) de $\Delta_{R,DF}$, alors cet arbre est sélectionné pour être étudié par la suite.

Pour calculer $\Delta_{R,DF}|_{A.E._i}$, le FDR de l'initiateur de chaque arbre d'événements est estimé avec le modèle compact et avec le modèle complet. La contribution de chaque arbre à $\Delta_{R,DF}$ se calcule comme :

$$\frac{\Delta_{R,DF}|_{A.E._i}}{\Delta_{R,DF}} = \frac{FDR\left(Initiateur_i\right)_{complet} \cdot R_{complet}}{\Delta_{R,DF}} - \frac{FDR\left(Initiateur_i\right)_{compacte} \cdot R_{compacte}}{\Delta_{R,DF}}$$

avec :

$FDR\left(Initiateur_i\right)_{complet}$ le FDR de l'initiateur i calculé avec le modèle complet. Si cet initiateur est modélisé au moyen d'un arbre de défaillances, ce FDR est un FDR étendu au niveau des fonctions (cf. 1.6 page 91),

$FDR\left(Initiateur_i\right)_{compacte}$ le FDR de l'initiateur i calculé avec le modèle compact.

Dans cette approche, un arbre d'événements est donc conservé si :

$$\frac{\Delta_{R,DF}|_{A.E._i}}{\Delta_{R,DF}} \geq Seuil$$

La valeur de ce seuil peut être, dans un premier temps, fixée à un niveau relativement haut, de manière à ne sélectionner que les arbres d'événements contenant les macro-coupes affectées par les plus grosses interdépendances significatives pour le risque. Une fois que ces interdépendances ont été supprimées, on peut recalculer $\frac{\Delta_{R,DF}|_{A.E._i}}{\Delta_{R,DF}}$. S'il reste trop élevé, on pourra diminuer la valeur de ce seuil pour prendre en compte plus d'arbres.

Identification des macro-coupes contenant des interdépendances significatives pour le risque : Pour identifier les macro-coupes qui contiennent des interdépendances pénalisantes pour le risque, on compare la probabilité de chaque macro-coupe des arbres d'événements sélectionnés à l'étape précédente avec sa probabilité estimée dans le modèle compact.

Toutefois, dans le modèle complet, on n'a pas directement accès à la probabilité des macro-coupes comme dans le modèle compact, dans lequel les coupes générées par le modèle correspondent aux macro-coupes. On peut en revanche, dans le modèle complet, identifier de manière automatique les coupes de référence correspondant à une macro-coupe, c'est-à-dire les coupes de référence dont l'occurrence implique celle de la macro-coupe. La probabilité d'une macro-coupe estimée à partir des coupes de référence du modèle complet se calcule donc comme :

$$P\left(Macro-coupe_i\right)_{complet} = P\left(\bigcup_{CM_k \in Macro-coupe_i} CM_k\right)$$

avec $Macro-coupe_i$ l'événement "occurrence de la macro-coupe i lors de l'exploitation de la centrale à l'étude" et CM_k une coupe de référence du modèle complet.

Dans notre étude, nous recherchons les interdépendances entre lignes de défense d'une même macro-coupe qui pèsent sur le risque. Le fait que deux lignes de défense soient interdépendantes n'est pas un problème en soi (même si elles sont dans la même macro-coupe). C'est pour cette raison qu'on ne considère que les coupes minimales pour estimer la probabilité d'une macro-coupe. En effet, les coupes non-minimales qui correspondent à des modes communs fonctionnels n'ont aucun impact sur le risque. C'est le cas dans l'exemple suivant.

Exemple : Si on étudie la macro-coupe $Initiateur \cap LD_1 \cap LD_3$ de la figure 4.5, on se rend compte que les lignes de défense 1 et 3 ne sont pas indépendantes. En effet, elles contiennent toutes deux EB_3. Cette interdépendance n'a pourtant aucun impact sur le risque car la coupe $Init_2 \cap EB_3 \cap EB_4$ qui contient cette interdépendance n'est pas minimale.

Pour comparer la probabilité d'une macro-coupe dans le modèle complet et dans le modèle compact, on compare donc la probabilité de la macro-coupe directement estimée dans le modèle compact avec la probabilité de l'ensemble des coupes de références correspondant à cette macro-coupe dans le modèle complet. Pour chaque macro-coupe i, notre indicateur est donc :

$$\frac{P\left(Macro-coupe_i\right)_{complet} - P\left(Macro-coupe_i\right)_{compacte}}{\Delta_{R,DF}}.$$

Si cette valeur est supérieure à un seuil, on doit identifier et supprimer les interdépendances entre les lignes de défense de cette macro-coupe.

Initiateur	Ligne de défense 1 LD_1	Ligne de défense 2 LD_2	Ligne de défense 3 LD_3	Conseq.
$Init_2$	$EB_1 \cup (EB_3 \cap EB_4)$	EB_3	$EB_2 \cup EB_3$	
			1	CA
			2	CI
			3	CA
			4	CI
			5	CI

Fig. 4.5 – *Exemple d'arbre d'événement*

Exemple de mesure des interdépendances au sein d'une macro-coupe : Dans l'exemple de la figure 4.1 page 115, la première macro-coupe s'exprime comme $Initiateur \cap LD_1$. Dans le modèle compact, elle correspond à la macro-coupe $EB_{init} \cap EB_{LD_1}$. Dans le modèle complet, elle correspond aux deux coupes de référence : $(Init_1 \cap EB_1)$, $(Init_1 \cap EB_2)$. Pour comparer la probabilité de cette macro-coupe selon que l'on prend, ou non, en compte les interdépendances entre lignes de défense, on calcule :

$$\frac{\overbrace{P\left((Init_1 \cap EB_1) \cup (Init_1 \cap EB_2)\right)}^{P(Initiateur \cap LD_1)_{complet}} - \overbrace{P\left(EB_{init} \cap EB_{LD_1}\right)}^{P(Initiateur \cap LD_1)_{compact}}}{\Delta_{R,DF}}.$$

Si cette valeur est supérieure à un seuil fixé, on devra identifier les causes des causes communes fonctionnelles.

Causes des interdépendances, identification des systèmes interdépendants : Au sein de chaque macro-coupe contenant des interdépendances non négligeables pour le risque, on peut chercher les lignes de défense qui sont interdépendantes. Pour ce faire, on calcule :

$$\frac{P\left(LD1 \cap LD2\right)}{P\left(LD1\right) \cdot P\left(LD2\right)}$$

Si ce ratio est supérieur à un, alors ces deux systèmes partagent des causes communes fonctionnelles.

Toutefois, deux lignes de défense d'une même macro-coupe peuvent être interdépendantes sans que cette interdépendance ait un quelconque impact sur le risque de référence. Cette mesure de l'interdépendance entre deux lignes de défense nous donne juste une indication sur les interdépendances pouvant expliquer l'écart entre $P\left(Macro-coupe_i\right)_{complet}$ et $P\left(Macro-coupe_i\right)_{compact}$.

Exemple : Comme on l'a vu dans l'exemple de la figure 4.5, les lignes de défense 1 et 3 ne sont pas indépendantes. Ainsi,

$$\frac{P\left(LD_1 \cap LD_3\right)}{P\left(LD_1\right) \cdot P\left(LD_3\right)} > 1.$$

En effet, elles contiennent toutes deux EB_3. Cette interdépendance n'a pourtant aucun impact sur le risque car la coupe $Init_2 \cap EB_3 \cap EB_4$ qui contient cet EB commun aux deux lignes de défense n'est pas minimale.

Deux lignes de défense d'une même macro-coupe (la macro-coupe $Initiateur \cap LD_1 \cap LD_3$) peuvent donc être interdépendantes sans que cette interdépendance ait un impact sur la différence entre $P\left(Macro-coupe_i\right)_{complet}$ et $P\left(Macro-coupe_i\right)_{compact}$.

Causes des interdépendances, identification des matériels partagés : Savoir quelles lignes de défense de la macro-coupe étudiée sont interdépendantes peut être une information insuffisante. Il nous semble utile de connaître les événements élémentaires qui sont source de ces interdépendances au sein de la macro-coupe i. Pour ce faire, on identifie tous les EB_j appartenant à plusieurs lignes de défense de la macro-coupe i. Puis, on calcule la probabilité de chaque coupe de référence associée à la macro-coupe i, en faisant l'hypothèse que l'EB_j est différent dans chaque ligne de défense. On fait donc l'hypothèse de diversification de l'EB_j. Enfin, on compare la probabilité de l'union de toutes ces coupes avec et sans l'hypothèse de diversification. On utilise alors le Facteur de Diminution de Risque dû à une Diversification de EB_j dans la macro-coupe i. On note cet indicateur $FDRD\left(EB_j\right)_{Ma.-coupe_i}$:

$$FDRD\left(EB_j\right)_{Ma.-coupe_i} = \frac{P\left(Macro-coupe_i\right)_{complet} - \overbrace{P\left(Macro-coupe_i\right)_{diversification\ EB_j}}^{\text{La prob. de la macro-coupe lorsque } EB_j \text{ est diversifié dans toutes les lignes de déf.}}}{P\left(Macro-coupe_i\right)_{complet}}$$

Si cet indicateur est proche de 100%, l'EB dont on fait l'hypothèse qu'il est diversifié génère la plus grande part de l'accroissement de la probabilité de la macro-coupe i dû aux interdépendances. Il est alors très intéressant de diversifier les matériels partagés qui correspondent à cet EB. Si l'indicateur est proche de zéro, il y a peu d'intérêt à diversifier cet EB. Après la diversification des matériels partagés (correspondant aux EB créant des interdépendances), le modèle EPS complet doit être remis à jour pour intégrer ces modifications. De même, la probabilité d'occurrence des macro-événements du modèle compact doit être remise à jour.

Exemple : Prenons l'exemple de l'arbre d'événements de la figure 4.6.

Initiateur	Ligne de défense 1 LD_1	Ligne de défense 2 LD_2	Ligne de défense 3 LD_3	Conseq.
$Init_3$	$EB_1 \cup (EB_3 \cap EB_4)$	$EB_3 \cap EB_5$	$EB_2 \cup EB_3 \cup (EB_1 \cap EB_5)$	
			1	CA
			2	CI
			3	CA
			4	CI
			5	CI

FIG. 4.6 – *Exemple d'arbre d'événements*

TAB. 4.1 – *Probabilité d'occurrence des différents événements de base*

EB	$Init_3$	EB_1	EB_2	EB_3	EB_4	EB_5
Probabilité	10^{-2}	10^{-7}	10^{-7}	10^{-2}	10^{-2}	10^{-2}

Si, dans cet exemple, on cherche à déterminer le ou les EB causant des modes communs au sein de la macro-coupe $Initiateur \cap LD_1 \cap LD_3$, on fait la liste des EB présents dans plusieurs lignes de défense de la macro-coupe, c'est-à-dire ici EB_1 et EB_3. Ensuite, on identifie les coupes de référence correspondant à cette macro-coupe. Ce sont les suivantes :

$$\left(Init_3 \cap EB_1 \cap EB_2\right),\ \left(Init_3 \cap EB_1 \cap EB_3\right),\ \left(Init_3 \cap EB_3 \cap EB_4\right) \text{ et } \left(Init_3 \cap EB_1 \cap EB_5\right)$$

Ensuite, on pose l'hypothèse que EB_1 est différencié entre les lignes de défense 1 et 3. L'EB_1 est alors l'$EB_{1,LD1}$ et l'$EB_{1,LD3}$. Les coupes correspondant à la macro-coupe étudiée sont alors

$$(Init_3 \cap EB_{1,LD1} \cap EB_2)\,,\ (Init_3 \cap EB_{1,LD1} \cap EB_3)\,,\ (Init_3 \cap EB_3 \cap EB_4)$$
$$\text{et}\ \ (Init_3 \cap EB_{1,LD1} \cap EB_{1,LD3} \cap EB_5)$$

Enfin, on pose l'hypothèse que EB_3 est différencié entre les lignes de défense 1 et 3. L'EB_3 est alors l'$EB_{3,LD1}$ et l'$EB_{3,LD3}$. Les coupes correspondant à la macro-coupe étudiée sont alors

$$(Init_3 \cap EB_1 \cap EB_2)\,,\ (Init_3 \cap EB_1 \cap EB_{3,LD3})\,,\ (Init_3 \cap EB_1 \cap EB_5)\,,$$
$$(Init_3 \cap EB_{3,LD1} \cap EB_2 \cap EB_4)\ \ \text{et}\ \ (Init_3 \cap EB_{3,LD1} \cap EB_{3,LD3} \cap EB_4)$$

On trouve donc que dans la macro-coupe $Initiateur \cap LD_1 \cap LD_3$:

$$FDRD\,(EB_1) = 0\%\ \text{et}\ FDRD\,(EB_3) = 99\%$$

Il est donc intéressant de diversifier EB_3 et non pas EB_1.

Causes des interdépendances, identification des coupes de référence contenant un grand nombre de modes communs fonctionnels : Un accroissement de risque important peut être dû à un ensemble de plusieurs interdépendances de faible importance entre lignes de défense, où chaque composant peut ne jouer qu'un rôle restreint dans ces modes communs fonctionnels.

Les indicateurs que nous avons proposés précédemment reposent sur l'identification des composants partagés, ou sur l'identification des lignes de défense interdépendantes deux à deux au sein d'une même macro-coupe. Ils sont donc impuissants à détecter un important accroissement de risque dû aux interdépendances lorsque cet accroissement est dû à de multiples petites interdépendances entre chacune des lignes de défense de la macro-coupe.

C'est le cas dans l'exemple suivant. Supposons qu'on étudie une macro-coupe $Initiateur_4 \cap LD_1 \cap LD_2 \cap LD_3 \cap LD_4$. Supposons que le jeu de coupes de chaque ligne de défense soit : $LD_1 = EB_1 \cap EB_2$, $LD_2 = EB_2 \cap EB_3$, $LD_3 = EB_3 \cap EB_4$, $LD_4 = EB_4 \cap EB_1$.

Supposons que chaque événement de base ainsi que l'initiateur aient une probabilité d'occurrence de 10^{-1}. La seule coupe de référence correspondant à cette macro-coupe est :

$Init_4 \cap EB_1 \cap EB_2 \cap EB_3 \cap EB_4$. Cette coupe de référence a une probabilité d'occurrence de 10^{-5}, alors que la probabilité d'occurrence de la macro-coupe correspondante dans le modèle compact est estimée à 10^{-9}. Il y a donc un fort impact des modes communs fonctionnels. Pourtant, lorsqu'on fait l'hypothèse de diversification pour l'EB 1, 2, 3 ou 4, le risque passe de 10^{-5} à 10^{-6}. Aucun de ces EB ne peut expliquer à lui seul cet écart de risque.

Pour détecter ce type de cas, on estime la probabilité de chaque coupe de référence associée à la macro-coupe étudiée en faisant l'hypothèse de diversification de tous les événements de base partagés en même temps. Pour chaque coupe de référence j associée à la macro-coupe i, cette probabilité est approchée par :

$$P\left(CM_{i,\text{référence}}/\text{diversification complète}\right) \approx \prod_{LD_k \in Ma-cp_i} P\left(\bigcup_{\substack{CM_{h,k} \in LD_k \\ CM_{h,k} \subset CM_{i,\text{référence}}}} CM_{h,k}\right)$$

avec :

$CM_{h,k}$	une coupe minimale de l'événement "défaillance de la ligne de défense k" qui est incluse dans la coupe de référence $CM_{i,\text{référence}}$,
LD_k	la ligne de défense k qui appartient à la macro-coupe i.
$Ma-cp_i$	la macro-coupe étudiée

Dans les coupes pour lesquelles $P\left(CM_{i,\text{référence}}/\text{diversification complète}\right) \ll P\left(CM_{i,\text{référence}}\right)$, on doit diminuer le nombre de sous-fonctions partagées entre les lignes de défense de la macro-coupe à laquelle correspond $CM_{i,\text{référence}}$.

Modification pour diminuer les modes communs fonctionnels : Suite aux cinq étapes précédentes, l'utilisateur sait où se trouvent les modes communs fonctionnels et a les moyens d'en déduire les causes puisqu'au sein de chaque macro-coupe, il peut connaître la liste des systèmes interdépendants, la liste des composants causant ces modes communs fonctionnels et enfin la liste des coupes contenant un nombre élevé de modes communs fonctionnels qui contribuent à une forte augmentation du risque.

Les concepteurs sont alors en mesure de réduire le nombre de composants ou sous-systèmes utilisés par plusieurs lignes de défense. La démarche la plus intuitive serait de dédoubler les sous-systèmes partagés par deux lignes de défense pour ne plus avoir de modes communs fonctionnels. Si la ligne de défense i et la ligne de défense j partagent le sous-système k, on créerait donc un sous-système k_i pour la ligne de défense i et un sous-système k_j différent pour la ligne de défense j. Bien que dédoubler un système partagé soit simple et efficace, si ce sous-système k est dédoublé, la mise en parallèle de k_i et k_j peut être intéressante en termes de risque à condition que cette modification n'ajoute pas de modes communs fonctionnels significatifs.

Exemple : Supposons que la ligne de défense "injection aux joints des pompes primaires" et la ligne de défense "injection de sécurité" partagent la même pompe 1. Supposons que ces deux lignes de défense interviennent dans la même macro-coupe i. Supposons enfin que cette macro-coupe soit sélectionnée dans les macro-coupes contenant des modes communs fonctionnels pénalisants pour le risque. Suite à l'application de la démarche proposée dans ce document, la pompe 1 sera identifiée comme source de cette interdépendance, comme le montre la figure 4.7

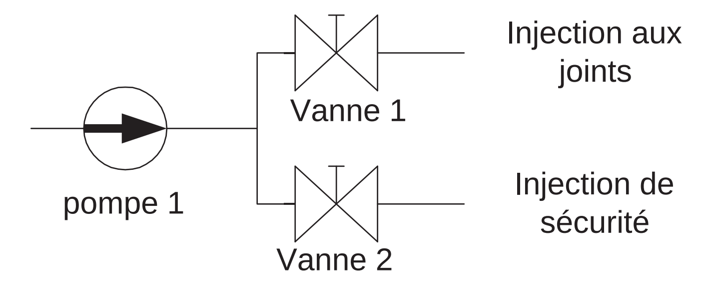


FIG. 4.7 – *Schéma de l'exemple avant modification*

Le premier réflexe est d'installer une pompe spécifique pour chaque fonction. On obtiendrait alors la figure 4.8.

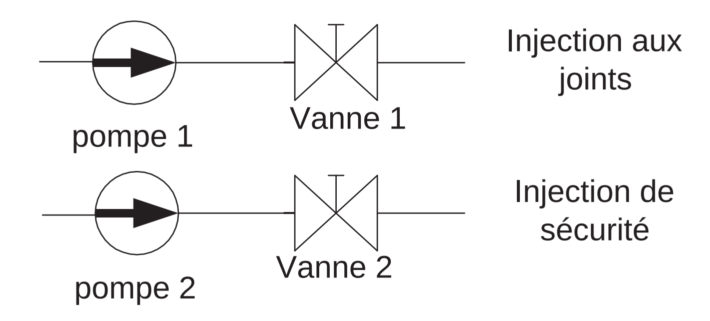


FIG. 4.8 – *Schéma de l'exemple après diversification des pompes*

Toutefois, on obtient un meilleur niveau de risque en mettant les deux pompes en parallèle, si leur mise en parallèle n'ajoute pas de mode commun fonctionnel. Ainsi, le design de la figure

4.9 sera plus avantageux que celui de la figure 4.8 si cette mise en parallèle n'ajoute pas des modes communs tels que l'ouverture intempestive de la vanne 2 (alors que l'injection de sûreté n'est pas requise), qui entraînerait une diminution importante du débit de l'injection aux joints.

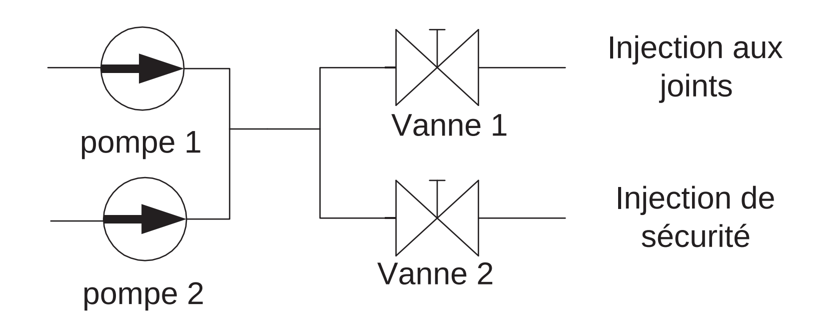


Fig. 4.9 – *Schéma de l'exemple après mise en parallèle des pompes*

3.4 Défense en profondeur et interdépendances significatives pour la sûreté

L'approche de la défense en profondeur que nous proposons dans cette section s'inspire de l'approche "*rationnelle*" proposée par Sorensen dans [81].

Objectif

Grâce aux étapes présentées dans la section précédente (3.3), l'importance des modes communs fonctionnels contribuant fortement au risque a été diminuée. Toutefois, tous les modes communs fonctionnels n'ont pas été supprimés. En effet, un composant très fiable peut être indispensable au fonctionnement de plusieurs lignes de défense, qu'elles appartiennent ou non à la même macro-coupe. Puisque ce composant est très fiable, le mode commun fonctionnel qu'il génère ne pèse pas dans le risque. Cependant, si ce composant venait à défaillir, l'impact sur le risque serait très important,

- soit parce que ce composant participe au fonctionnement de très nombreuses lignes de défense qui ne sont pas dans les mêmes macro-coupes. Ce composant est alors intrinsèquement important et on assiste en cas de défaillance à un augmentation simultanée de la probabilité d'occurrence de nombreuses macro-coupes ;
- soit parce que ce composant participe au fonctionnement de plusieurs lignes de défense d'une même macro-coupe. Ce composant génère alors un mode commun fonctionnel au sein de cette macro-coupe et en cas de défaillance, la probabilité d'occurrence de cette macro-coupe augmente fortement.

Ce sont ces modes communs fonctionnels "dormants" minant la défense en profondeur qui sont recherchés et supprimés dans cette partie. En effet, on est sûr à ce stade de n'avoir plus que des modes communs fonctionnels "dormants" car ceux qui pesaient sur le risque ont été réduits dans l'étape précédente.

Méthode

Le traitement des modes communs fonctionnels significatifs pour la sûreté est réalisé en appliquant le critère de défaillance unique probabiliste au niveau des composants. Pour ce faire, on détermine tout d'abord les événements de base significatifs pour la sûreté (voir la définition de significatif pour la sûreté et significatif pour le risque proposée par Youngboold dans [100]). Ensuite, pour chacun des ces EB, on regarde dans quelles macro-coupes il pose problème. Enfin, on vérifie si, dans les macro-coupes sélectionnées, ces EB génèrent des modes

communs fonctionnels et, le cas échéant, on supprime ces modes communs. Dans le cas contraire, c'est-à-dire si ces EB ne génèrent pas de mode commun fonctionnel, les matériels associés à ces EB sont redondés là où ils sont les plus importants.

Identification des EB significatifs pour la sûreté : Pour détecter les EB qui sont significatifs pour la sûreté, on calcule l'accroissement de risque consécutif à la perte de chaque EB à partir du modèle complet.

$$Accroissement\ risque\ EB_i = FAR\,(EB_i) \cdot R_{complet}$$

Les EB dont l'occurrence implique un accroissement de risque supérieur à un seuil sont sélectionnés. L'occurrence certaine de ces EB peut impliquer un accroissement de risque important car ils interviennent dans de nombreuses lignes de défense et/ou dans de nombreux initiateurs qui ne sont pas dans les mêmes macro-coupes. Dans ce cas, l'occurrence de ces EB n'affaiblit qu'au plus une ligne de défense par macro-coupe. Le problème réside dans le fait que cette occurrence affaiblit simultanément de nombreuses lignes de défense et entraîne donc une augmentation simultanée de la probabilité d'occurrence de nombreuses macro-coupes. Les matériels associés à ces EB peuvent être diversifiés ou redondés au sein des lignes de défense où ils jouent leur plus grand rôle.

En revanche, si un EB joue un rôle important dans plusieurs lignes de défense (ou dans l'initiateur et dans au moins une ligne de défense) d'une même macro-coupe, on est face à une cause commune fonctionnelle dormante dont l'occurrence affaiblit plusieurs lignes de défense successives. On perd alors, du moins partiellement, la redondance des lignes de défense. Le matériel correspondant doit être diversifié entre les lignes de défense successives (c'est-à-dire entre les lignes de défense appartenant à la même macro-coupe) et, le cas échéant, l'initiateur.

Identification des causes communes "dormantes" : Pour voir si un EB_k important pour la sûreté génère des modes communs fonctionnels dormants au sein d'une même macro-coupe,

- on recherche les arbres d'événements où cet EB est important pour la sûreté. Pour cela, on calcule l'accroissement de risque quand l'EB_k est certain au sein de chaque arbre d'événements ;
- on recherche, au sein de ces arbres, les macro-coupes i où l'EB_k est important pour la sûreté. Pour cela, on calcule la probabilité des coupes associées à la macro-coupe i quand l'EB est considéré comme certain :

$$\begin{array}{c}\text{Accroissement lié à } EB_k \\ \text{dans macro-coupe } i\end{array} = P\left(\bigcup_{CM_{j,ref.} \in Ma-cp_i} CM_{j,ref.}/EB_k\right) - P\left(\bigcup_{CM_{j,ref.} \in Ma-cp_i} CM_{j,ref.}\right)$$

avec $CM_{j,ref.}$ une coupe du risque de référence associée à la macro-coupe i.

- Dans chacune de ces macro-coupes identifiées, on calcule l'accroissement de la probabilité d'occurrence de l'initiateur et la probabilité de défaillance de chacune de ses lignes de défense quand EB_k est certain en ne se basant que sur les coupes incluses dans les coupes de référence :

$$P\left(\bigcup_{\substack{CM_{h,Init.}\in Initiateur\\ CM_{h,Init.}\in CM_{l,ref.}}} CM_{h,Init.}/EB_k\right) - P\left(\bigcup_{\substack{CM_{h,Init.}\in Initiateur\\ CM_{h,Init.}\in CM_{l,ref.}}} CM_{h,Init.}\right)$$

avec $CM_{l,ref.} \in Macro - coupe_i$
et $Initiateur \in Macro - coupe_i$

$$P\left(\bigcup_{\substack{CM_{k,LD_j}\in LD_j\\ CM_{k,LD_j}\in CM_{l,ref.}}} CM_{k,LD_j}/EB_k\right) - P\left(\bigcup_{\substack{CM_{k,LD_j}\in LD_j\\ CM_{k,LD_j}\in CM_{l,ref.}}} CM_{k,LD_j}\right)$$

avec $CM_{l,ref.} \in Macro - coupe_i$
et $LD_j \in Macro - coupe_i$

avec $CM_{l,ref.}$ une coupe de référence, CM_{k,LD_j} une coupe associée à l'occurrence de la défaillance de la ligne de défense j et $CM_{k,Init.}$ une coupe associée à l'occurrence de l'initiateur de la macro-coupe i.

Si cet accroissement est important pour plusieurs lignes de défense d'une même macro-coupe ou pour l'initiateur et une ligne de défense au moins, alors l'occurrence de EB_i a un impact significatif pour plusieurs lignes de défense d'une même macro-coupe (et éventuellement pour l'initiateur). Le composant associé à EB_i doit être diversifié ou redondé entre les lignes de défense où il est important.

Si cet accroissement n'est important que pour une seule ligne de défense, alors on retient cette ligne de défense dans la liste des lignes de défense où le composant associé à l'EB étudié pourra être redondé. Si on ne peut ou on ne veut pas redonder le composant auquel se rapporte l'EB étudié, il faut diminuer l'importance de la ligne de défense où EB_k est important.

3.5 Critère de défaillance unique qualitatif

Objectif

Dans la section précédente, on a utilisé un critère de défaillance unique inspiré de la définition "*rationnelle*" de la défense en profondeur. Dans cette section, nous proposons d'utiliser l'approche "*structurelle*" de la défense en profondeur, proposée aussi par Sorensen [81], en appliquant notre critère de défaillance unique qualitatif au niveau des EB. On cherche à ce que, quel que soit l'événement considéré, son occurrence n'entraîne pas à elle seule celle de l'événement CI et ce, quel que soit l'initiateur considéré comme réalisé. Ce critère de défaillance qualitatif revient donc à vérifier qu'il n'existe pas de coupes de référence d'ordre inférieur ou égal à deux.

Contexte

Suite aux étapes précédentes, il ne doit y avoir que peu ou pas d'EB ne vérifiant pas ce critère. En effet, supposons qu'il existe une coupe $Init_1 \cap EB_1$. Le FAR du seul EB contenu dans cette coupe vaut $^{P(Init_1)}/_R$. Il doit être très élevé, à moins que $P(Init_1)$ ne soit très faible. Si le FAR de EB_1 est très élevé, cet EB a été redondé ou diversifié s'il affaiblissait plusieurs lignes de défenses successives. Cette approche structurelle n'est donc utile que pour détecter des problèmes de défense en profondeur liés à l'occurrence d'initiateurs très rares.

Méthode

On génère les coupes du modèle complet en y incluant les initiateurs "flous". (Leur probabilité ne doit plus être nulle, on leur attribue une valeur forfaitaire quelconque. Cette valeur n'a aucune importance puisqu'on applique ici une approche qualitative et non pas quantitative). Si le jeu de coupes doit être tronqué, le processus de troncation utilisé doit être un processus de troncation par ordre, de manière à être sûr d'avoir au moins toutes les coupes d'ordre deux,

quelle que soit leur probabilité d'occurrence.

S'il y a peu de coupes d'ordre deux, on redonde les quelques matériels qui correspondent aux événements de base appartenant à ces coupes ou on démontre, pour les coupes d'ordre deux que l'on ne veut pas modifier, le caractère très improbable de l'initiateur et sa totale indépendance avec le seul EB de la coupe.

S'il y a de nombreuses coupes d'ordre deux, on compte, pour chaque EB, le nombre de coupes d'ordre deux où il apparaît. On redondera en priorité les matériels correspondant aux EB qui participent le plus souvent à des coupes d'ordre deux. On peut aussi regrouper ces coupes par initiateur. On verra alors pour quels initiateurs il existe des problèmes de défense en profondeur. On pourra alors exceptionnellement envisager la création de nouvelles lignes de défense pour parer à ces initiateurs.

Suite à ces modifications, on met de nouveau à jour le modèle complet et les probabilités d'occurrence des macro-événements du modèle compact.

3.6 Composants et lignes de défense inutiles

Objectif

Durant les différentes étapes présentées précédemment, de nombreuses modifications ont été décidées. Du fait de ces modifications, mais aussi à cause de l'impact des dépendances fonctionnelles qui peuvent court-circuiter des lignes de défense dans certains contextes, des lignes de défense peuvent être devenues inutiles. Dans cette partie, le but est de détecter les lignes de défense et les composants inutiles, puis de les supprimer, le cas échéant.

Contexte

La conception de la centrale, lorsqu'on arrive à cette étape, valide tous les objectifs fixés en termes de risque résiduel ou de défense en profondeur. On peut donc, sans préjudice pour ces derniers, supprimer les lignes de défense et les composants inutiles. Il ne faut toutefois pas confondre avec ceux-ci les composants et lignes de défense dédiés à la gestion des initiateurs flous qui ne peuvent être considérés de manière qualitative.

Méthode

Identification des lignes de défense inutiles : Pour identifier une ligne de défense inutile, on calcule, pour la fonction de chaque ligne de défense, son FAR et son FDR (avec le FAR et le FDR étendus au niveau des fonctions, comme décrit dans la section 1.6 page 91 du chapitre 3). Si ces deux valeurs sont nulles, la ligne de défense, d'après le modèle EPS, ne sert à rien.

$$\underbrace{FAR(LD_i)_{Fonction}}_{=\frac{P(CI/LD_i\text{ existe plus})-P(CI)}{P(CI)}} = \underbrace{FDR(LD_i)_{Fonction}}_{\frac{P(CI)-P(CI/LD_i\text{ toujours remplie})}{P(CI)}} = 0$$

Suppression d'une ligne de défense : Une ligne de défense i (notée LD_i) est jugée inutile si elle vérifie l'ensemble des conditions suivantes :

1. $FAR(LD_i)_{Fonction} = FDR(LD_i)_{Fonction} = 0$
2. La suppression de la ligne de défense i ne produit pas de macro-coupe d'ordre deux. Si c'est le cas, on respecte bien le critère de défaillance unique qualitatif. Dans cette étape, il faut aussi considérer les arbres d'événements contenant des initiateurs flous. En effet, ce n'est pas parce qu'on ne peut pas quantifier la probabilité d'occurrence de ces initiateurs qu'ils ne doivent pas être considérés dans la défense en profondeur.
3. Le panel d'experts consulté est favorable à sa suppression.
4. Son coût de construction ou d'exploitation n'est pas négligeable.

Si une ligne de défense est jugée inutile, on peut supprimer du design de la centrale tous les composants n'étant utilisés que par la ligne de défense que l'on veut supprimer.

Identification des composants inutiles : La démarche est sensiblement la même. Pour prendre en compte les initiateurs flous dont on n'a pas pu définir la probabilité d'occurrence (elle vaut zéro par défaut dans le modèle complet), on les considère comme réalisés. On calcule alors le FAR[4] de chaque EB du modèle et son FDR. Si, pour un composant donné, tous les EB qui lui correspondent ont un FAR et un FDR nuls, alors ce composant paraît inutile à la lumière de l'EPS.

On doit donc calculer pour chaque EB :

$$FAR\left(EB_i/E_{1,PGT_{init\ flous}}\right) = \frac{P\left(CI/EB_i \cap E_{1,PGT_{init\ flous}}\right) - P\left(CI/E_{1,PGT_{init\ flous}}\right)}{P\left(CI/E_{1,PGT_{init\ flous}}\right)}$$

$$FDR\left(EB_i/E_{1,PGT_{init\ flous}}\right) = \frac{P\left(CI/E_{1,PGT_{init\ flous}}\right) - P\left(CI/\overline{EB_i} \cap E_{1,PGT_{init\ flous}}\right)}{P\left(CI/E_{1,PGT_{init\ flous}}\right)}$$

avec $E_{1,PGT_{init\ flous}} = \bigcap_{Init_j = \substack{init.\ flou \\ inquantifiable}} Init_j$.

$E_{1,PGT_{init\ flous}}$ correspond à l'événement associé au groupe PGT contenant tous les initiateurs flous dont on ne peut définir la probabilité d'occurrence.

Suppression d'un composant : Un composant peut être supprimé à la triple condition qu'il apparaisse comme inutile dans l'EPS complète, qu'il ne soit dans aucune coupe d'ordre inférieur ou égal à deux (y compris lorsque les initiateurs flous sont pris en compte) et que tous les experts le jugent inutile. Dans ce cas, on peut supprimer ce composant du design de la centrale.

[4] Il faut prendre en compte les erreurs liées aux seuils de troncature lors du calcul des FAR et FDR : un FAR que l'on croit nul ne l'est pas forcément.

3.7 Schéma global de la démarche

Le figure 4.10 résume la démarche de prise en compte des interdépendances entre lignes de défense.

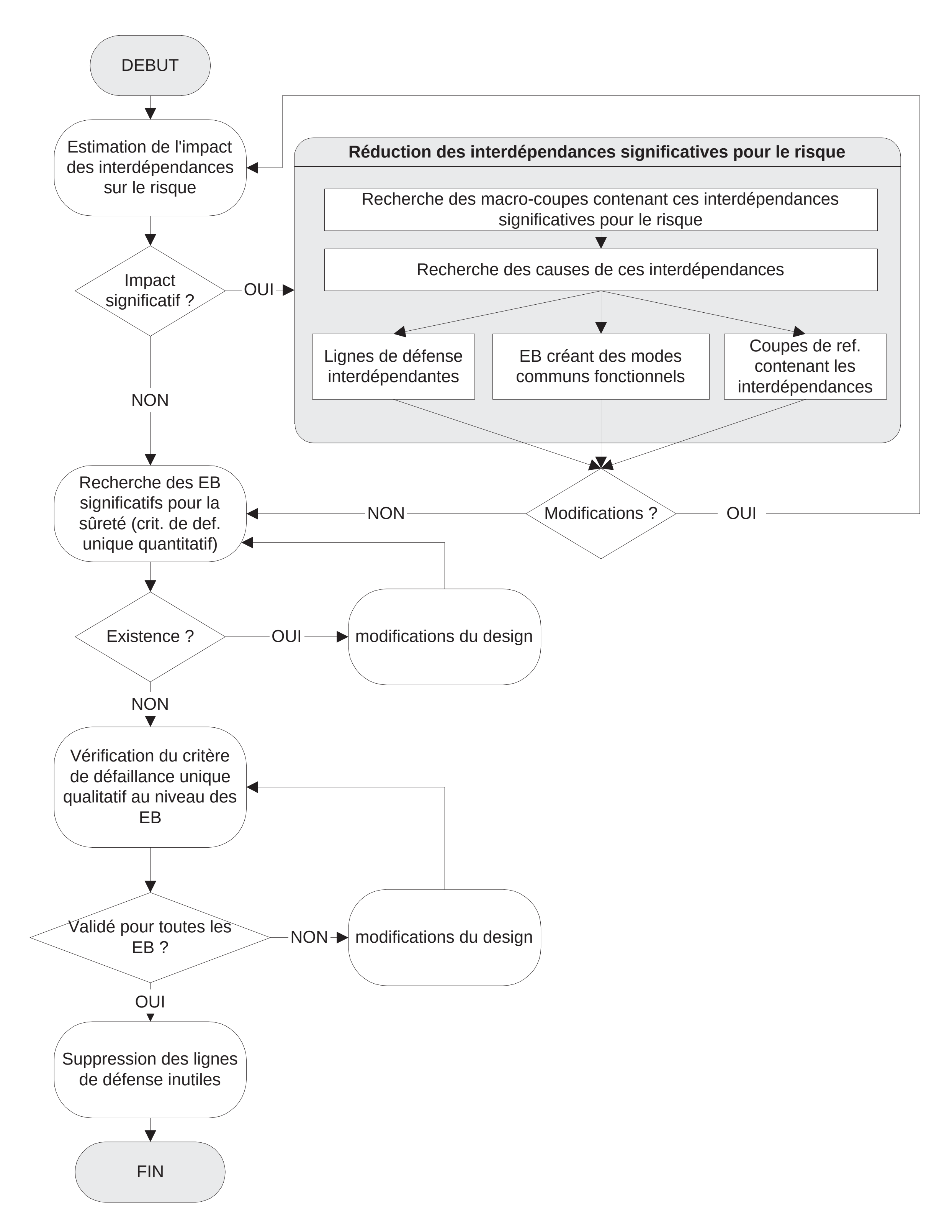


FIG. 4.10 – *Schéma global de la démarche de prise en compte des interdépendances*

3.8 Exemple d'application

3.8.1 Introduction de l'exemple illustratif

Dans cet exemple, on suppose que l'on étudie une centrale à eau sous pression très simplifiée et très "mal conçue". La partie de la centrale que l'on étudie est schématisée dans la figure 4.11. Le système ASG a pour fonction de refroidir le circuit primaire. Les systèmes d'Injection de Sécurité Haute pression (ISHP) ou Moyenne Pression (ISMP) ou Basse Pression (ISBP) ont pour fonction d'assurer l'appoint en eau en cas de brèche dans le circuit primaire. Ces trois fonctions diffèrent par leur mode d'action. L'ISMP est un système passif qui se déclenche lorsque la pression passe au-dessous d'un certain niveau, alors que l'ISHP et l'ISBP sont des systèmes actifs reposant sur la mise en marche de pompes, l'ouverture de vannes, etc. Ces deux dernières fonctions diffèrent par leur pression et leur débit de sortie. L'ISHP peut injecter de l'eau dans le circuit primaire sans qu'il soit dépressurisé, contrairement à l'ISBP.

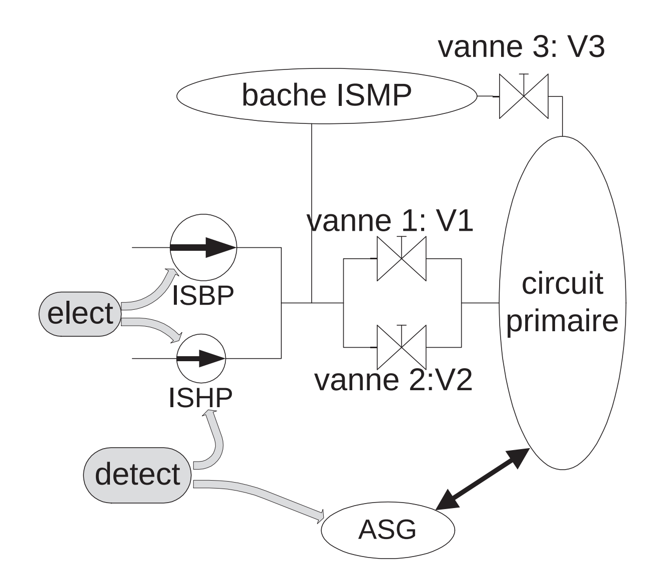


Fig. 4.11 – *Schéma de l'exemple*

Supposons que le seul initiateur qui puisse se produire soit "une petite fuite dans le circuit primaire" et que l'on se place dans le cadre d'une EPS de niveau I. L'événement redouté est donc la fusion d'un ou de plusieurs crayons de combustible. L'analyse fonctionnelle est la suivante. Supposons qu'une fuite se produise. Si elle est isolée avant une heure, la fusion est évitée. Si elle est non isolée, l'ISHP et l'ASG démarrent automatiquement. Si l'ISHP fonctionne, la fuite est compensée et la fusion évitée (que les autres lignes de défense fonctionnent ou non). Sinon, les opérateurs doivent réaliser une procédure de refroidissement maximum au moyen de l'ASG, pour dépressuriser rapidement le circuit primaire et pouvoir utiliser l'ISMP et l'ISBP. Si cette procédure est pas ou mal appliquée, ou si l'ISMP ou l'ISBP défaillent, on ne peut pas éviter la fusion du cœur.

Les EB associés à ces événements sont :

$Isol$ l'événement "échec de l'isolement de la brèche". $P(Isol) = 10^{-1}$

$elect_1$ l'événement "défaillance de l'alimentation électrique". $P(elect_1) = 10^{-5}$

$detect$ l'événement "détection automatique de la brèche". $P(detect) = 10^{-10}$

V_i l'événement "refus d'ouverture de la vanne i". $P(V_i) = 10^{-3}$

IHP l'événement "défaillance intrinsèque de l'injection haute pression". $P(IHP) = 10^{-5}$

IBP l'événement "défaillance intrinsèque de l'injection basse pression". $P(IBP) = 10^{-5}$

ASG l'événement "défaillance intrinsèque du système de refroidissement de secours". $P(ASG) = 10^{-7}$

RfM l'événement "échec du refroidissement maximum". $P(RfM) = 10^{-2}$

L'arbre d'événements correspondant à cet exemple est celui de la figure 4.12. Il correspond à l'analyse fonctionnelle que nous venons de décrire.

Petite brèche *Init*	Brèche isolée *LD*1	ISHP *LD*2	ASG *LD*3	Ref. Max. *LD*4	ISMP *LD*5	ISBP *LD*6		conseq.
							1	CA
							2	CA
							3	CA
							4	CI
							5	CI
							6	CI
							7	CI

FIG. 4.12 – *Arbre d'événements associé à l'exemple*

Les coupes correspondant à chaque mission de sauvegarde de l'arbre d'événements de la figure 4.12 sont présentées dans la table 4.2. La coupe correspondant à l'occurrence de l'initiateur est *Init*.

Ligne de déf.	coupes	ligne de déf.	coupes
Brèche isolée	$Isol$	Ref. Max.	RfM
ISHP	$eltc_1 \cup detect \cup V_1 \cap V_2 \cup IHP$	ISMP	$V_1 \cap V_2 \cap V_3$
ASG	$detect \cup ASG$	ISBP	$eltc_1 \cup V_1 \cap V_2 \cup IBP$

TAB. 4.2 – *Coupes des missions de sauvegarde de l'exemple*

3.8.2 Application de notre approche à cet exemple

Estimation de l'impact global des interdépendances sur le risque

$\Delta_{R,DF}$ est calculé à partir de l'estimation du risque donnée par le modèle complet et celle donnée par le modèle compact :

$$\Delta_{R,DF} = 1,11 \cdot 10^{-6} - 2,1 \cdot 10^{-8} = 1,089 \cdot 10^{-6}$$

Supposons qu'on souhaite concevoir une centrale dont le risque résiduel soit de l'ordre de 10^{-7}. On voit alors que $\Delta_{R,DF}$ est trop élevé. Il faut donc réduire les interdépendances qui pèsent sur le risque.

Interdépendances significatives pour le risque

Identification des arbres d'événements contenant des interdépendances significatives pour le risque : Dans la mesure où notre exemple ne comporte qu'un arbre d'événements, cet arbre représente forcément 100% des interdépendances. On fera donc l'hypothèse qu'il est significatif dans cette phase de recherche des arbres d'événements contenant des interdépendances significatives pour le risque.

Identification des macro-coupes contenant des interdépendances significatives pour le risque : Le modèle compact nous donne directement les macro-coupes. A partir de la figure 4.12 et de la table 4.2, on trouve les coupes de référence, qui sont :

$$\underbrace{(Init \cap Isol \cap elect_1) \cup (Init \cap Isol \cap V_1 \cap V_2) \cup (Init \cap Isol \cap IHP \cap IBP)}_{\text{coupes de référence correspondant à la macro-coupe 1}}$$
$$\cup \underbrace{(Init \cap Isol \cap IHP \cap RfM)}_{\text{coupes de référence correspondant à la macro-coupe 3}}$$
$$\cup \underbrace{(Init \cap Isol \cap IHP \cap ASG) \cup (Init \cap Isol \cap detect)}_{\text{coupes de référence correspondant à la macro-coupe 4}}$$

A partir des coupes de référence associées à leur macro-coupe d'origine et de la probabilité de chaque macro-coupe issue du modèle compact, on peut construire la table 4.3.

Macro-coupe numéro :	expression de la macro-coupe	Probabilité des coupes de référence correspondant à la macro-coupe (modèle complet)	Probabilité de la macro-coupe estimée avec le modèle compact
1	$Initiateur \cap LD_1 \cap LD_2 \cap LD_6$	$1,1 \cdot 10^{-6}$	$4,41 \cdot 10^{-11}$
2	$Initiateur \cap LD_1 \cap LD_2 \cap LD_5$	0	$2,1 \cdot 10^{-15}$
3	$Initiateur \cap LD_1 \cap LD_2 \cap LD_4$	10^{-8}	$2,1 \cdot 10^{-8}$
4	$Initiateur \cap LD_1 \cap LD_2 \cap LD_3$	$1,01 \cdot 10^{-11}$	$2,1 \cdot 10^{-13}$

TAB. 4.3 – *Différence entre modèle compact et modèle complet par macro-coupe*

La macro-coupe 2 a une probabilité nulle dans le modèle complet car aucune coupe de référence ne correspond à cette macro-coupe. En effet, l'événement CI est déjà réalisé avant qu'on ait atteint les conditions nécessaires à la réalisation de cette macro-coupe. Ainsi, la macro-coupe 2 s'exprime comme : $Initiateur \cap LD_1 \cap LD_2 \cap LD_5$. Si cette macro-coupe est considérée seule, il en résulte une coupe minimale qui est : $Init \cap Isol \cap V_1 \cap V_2 \cap V_3$. Cette coupe n'est plus minimale quand on calcule le risque de référence car la macro-coupe 1 produit la coupe $Init \cap Isol \cap V_1 \cap V_2$, qui est plus courte.

Ces résultats nous indiquent que la première macro-coupe contient des interdépendances significatives pour le risque. En effet,

$$\frac{P\left(\bigcup_{CM_{i,ref.} \in Macro-coupe_1} CM_{i,ref.}\right) - P\left(Ma - cp_1\right)_{\text{modèle compact}}}{\Delta_{R,FD}} = 1,01$$

Un résultat plus surprenant est le fait que certaines macro-coupes ont une probabilité d'occurrence plus élevée avec le modèle compact qu'avec le modèle complet. Cela est dû au fait que toutes les coupes minimales correspondant à une macro-coupe ne sont pas forcément des coupes de référence, car elles peuvent ne plus être minimales quand on considère ensemble toutes les coupes de toutes les macro-coupes.

Lorsqu'on considère par exemple l'événement $Macro - coupe_3$ seul, on constate qu'il correspond entre autres aux coupes $(Init \cap Isol \cap V_1 \cap V_2 \cap RfM)$, $(Init \cap Isol \cap elect_1 \cap RfM)$ et $(Init \cap Isol \cap detect \cap RfM)$. Ces coupes ne sont plus minimales lorsqu'on considère le risque de référence car d'autres macro-coupes correspondent aux coupes $(Init \cap Isol \cap V_1 \cap V_2)$, $(Init \cap Isol \cap elect_1)$ et $(Init \cap Isol \cap detect)$

Causes des interdépendances, identification des systèmes interdépendants : Dans la macro-coupe 1, sélectionnée parce qu'elle contient des interdépendances significatives pour le risque, on recherche les systèmes interdépendants :

$$\frac{P\left(LD_1 \cap LD_2\right)}{P\left(LD_1\right) \cdot P\left(LD_2\right)} = 1, \quad \frac{P\left(LD_1 \cap LD_6\right)}{P\left(LD_1\right) \cdot P\left(LD_6\right)} = 1, \quad \frac{P\left(LD_2 \cap LD_6\right)}{P\left(LD_2\right) \cdot P\left(LD_6\right)} = 2,49 \cdot 10^4$$

On voit alors que les lignes de défense 2 et 6 sont interdépendantes car notre indicateur vaut bien plus de 1. On a donc $P\left(LD_2/LD_6\right) \gg P\left(LD_2\right)$.

Causes des interdépendances, identification des matériels partagés : On recherche maintenant les EB qui peuvent être source de ces interdépendances. Les coupes de référence correspondant à la macro-coupe 1 sont : $Init \cap Isol \cap elect_1$, $Init \cap Isol \cap V_1 \cap V_2$ et $Init \cap Isol \cap IBP \cap IHP$.

Quand, par exemple, on fait l'hypothèse de diversification pour l'événement de base $elect_1$, la probabilité d'occurrence de la macro-coupe est approchée par :

$$P(Init) \cdot P(Isol) \cdot P(elect_1)^2 + P(Init) \cdot P(Isol) \cdot P(elect_1) \cdot P(IBP) \\ + P(Init) \cdot P(Isol) \cdot P(elect_1) \cdot P(detect) + P(Init) \cdot P(Isol) \cdot P(V_1) \cdot P(V_2) \\ + P(Init) \cdot P(Isol) \cdot P(elect_1) \cdot P(IHP) + P(Init) \cdot P(Isol) \cdot P(IBP) \cdot P(IHP)$$

Dans les faits, l'application informatique en charge d'estimer cette valeur devra prendre en compte le fait qu'une coupe de référence puisse correspondre à plusieurs macro-coupes. Dans ce cas, le gain résultant d'une diversification peut être moindre en termes de risque.

Suite à l'application de l'hypothèse de diversification successivement à tous les EB des lignes de défense de la macro-coupe 1, on trouve que $elect_1$, V_1 et V_2 sont source d'interdépendances.

Causes des interdépendances, identification des coupes de référence contenant un grand nombre de modes communs fonctionnels : L'hypothèse de diversification complète est faite coupe par coupe pour détecter les coupes de référence qui contiennent de gros modes communs fonctionnels. Par exemple, pour la coupe $Init \cap Isol \cap V_1 \cap V_2$ de la macro-coupe 1, l'application de l'hypothèse de diversification totale nous donne :

$$P(CM)_{\text{diversificat tot.}} = P(Init \cap Isol \cap (V_1 \cap V_2) \cap (V_1' \cap V_2'))$$

et on en déduit que :

$$\frac{P(CM) - P(CM)_{\text{diversificatř tot.}}}{\Delta_{R,DF}} = 0,1$$

Cette coupe ne contient donc pas énormément de modes communs fonctionnels significatifs pour le risque.

Modification pour diminuer les modes communs fonctionnels : Après cette analyse, une deuxième alimentation électrique fonctionnellement identique à la première mais techniquement différente, de façon à éviter les modes communs, est créée pour fournir en énergie l'ISBP et l'ISHP. Les vannes 1 et 2 doivent aussi être diversifiées. On crée donc une vanne 4 que l'on place en parallèle des vannes 1 et 2. Les modes communs fonctionnels entre ISHP et ISBP existent toujours mais sont de faible importance.

Interdépendances significatives pour la sûreté

Après la mise à jour du modèle suite aux modifications décidées à l'étape précédente, seul un événement de base a un FAR élevé, c'est *detect*. On se pose alors la question de savoir si cet EB peut correspondre à un mode commun fonctionnel dormant. Il faut donc rechercher les macro-coupes où il est présent dans plusieurs lignes de défense. Il n'y en a qu'une, la macro-coupe 4. On regarde alors si l'accroissement de la probabilité de défaillance de la ligne de défense i est important lorsque l'événement *detect* est certain, et ce quel que soit i appartenant à la macro-coupe 4. On se rend alors compte que l'occurrence de l'événement *detect* implique la défaillance des lignes de défense 2 et 3. Cet EB correspond donc bien à un mode commun fonctionnel dormant. Par conséquent, il faut traiter ce problème de défense en profondeur en diversifiant les moyens de détection entre le démarrage de l'ISHP (LD_2) et le démarrage de l'ASG (LD_3). La nouvelle conception de la centrale est alors celle de la figure 4.13. Elle intègre des modifications diminuant les causes communes fonctionnelles qui pèsent sur le risque (dédoublement des alimentations électriques, ajout de la vanne 4) et d'autres réduisant les causes communes graves pour la sûreté (ajout d'un deuxième moyen de détection).

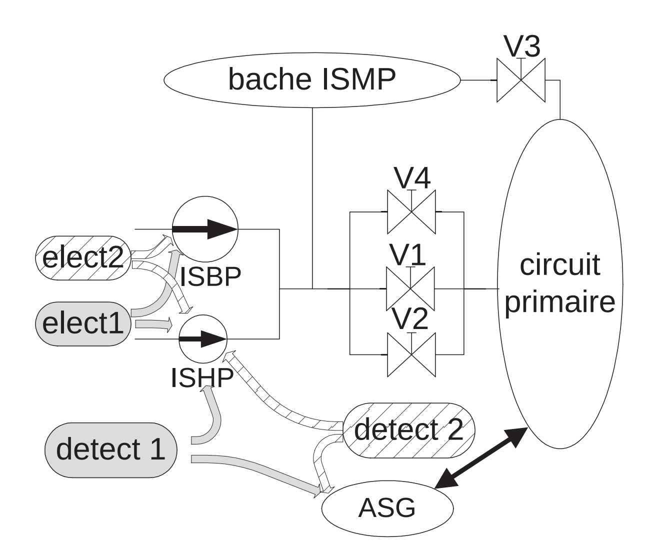


FIG. 4.13 – *Schéma de la conception à l'étude après diversification des sous-systèmes partagés*

Le nouveau risque correspondant à cette nouvelle conception est estimé après mise à jour du modèle complet. Il est de $R_{complet} = 1,012 \cdot 10^{-8}$.

Vérification du critère de défaillance unique qualitatif au niveau des EB :
Il n'existe aucune coupe de référence d'ordre deux. Ce critère est donc bien validé.

Détection des matériels et des lignes de défense "inutiles"
Lignes de défense inutiles : Supposons que l'on étudie la ligne de défense 5 (ISMP). Lorsque l'on calcule pour la ligne de défense 5 ($LD5$) le FDR, étendu au niveau des fonctions[5], on se rend compte qu'il est nul.

$$FDR\,(LD5)_{Fonction} = \frac{P\,(CI) - P\,(CI/LD5 \text{ impossible})}{P\,(CI)} = 0$$

Cela signifie que lorsque l'événement en tête $LD5$ est considéré comme impossible, le risque est inchangé. En effet, seule la macro-coupe 2 contient l'occurrence de cet événement en tête et il n'y a aucune coupe de référence correspondant à cette macro-coupe. En effet, toutes les coupes correspondant à l'occurrence de cette macro-coupe sont rendues non-minimales par la coupe de référence $Init. \cap Isol. \cap V_1 \cap V_2$ qui correspond à l'une des coupes de la macro-coupe 1.

On peut donc penser que cette ligne de défense est inutile, mais lorsqu'on calcule le FAR de sa fonction, on se rend compte que le risque est presque doublé lorsque cette fonction n'existe plus :

$$FAR\,(LD5)_{Fonction} = \frac{P\,(CI/LD5 \text{ existe plus}) - P\,(CI)}{P\,(CI)} = 0,9$$

Cette ligne de défense n'est donc pas inutile.

Matériels inutiles : Supposons que l'on étudie la vanne 3. Sa défaillance est modélisée par un seul EB, qui est V_3. Le FAR et le FDR de cet EB sont nuls. En effet, aucune coupe de référence ne contient l'événement V_3.

Ce résultat s'explique par le fait que la vanne 3 permet le fonctionnement de l'ISMP lorsque les vannes 1, 2 et 4 sont bloquées fermées. Toutefois, le fonctionnement de l'ISMP et de l'ISBP est nécessaire pour atteindre les conséquences acceptables. La vanne 3, qui permet le fonctionnement de l'ISMP lorsque l'ISBP est indisponible du fait de la non-ouverture des vannes 1, 2 et

[5]cf. section 1.6 page 91 du chapitre 3

4, est donc inutile. Du point de vue de notre EPS de niveau 1 ou 3, on peut la supprimer. Toutefois, les experts peuvent s'opposer à une telle suppression car même si le bon fonctionnement de l'ISMP ne suffit pas à lui seul à éviter la fusion, il peut diminuer la gravité des conséquences après la fusion[6].

Conclusion sur cet exemple

Suite à l'application de la démarche que nous proposons pour réduire les interdépendances fonctionnelles entre lignes de défense, la conception de chacune d'elle peut être modifiée. Après cette phase de re-conception de chaque ligne de défense, toutes les interdépendances ne sont pas supprimées. En effet, dans notre exemple, l'ISBP, l'ISHP et l'ASG partagent les mêmes alimentations électriques. Toutefois, ces interdépendances sont réduites parce que les systèmes partagés ont été rendondés de telle sorte qu'elles ne pèsent plus sur le risque et qu'un bon niveau de défense en profondeur est atteint.

4 Conclusion sur notre approche de conception

La méthodologie présentée dans ce document, parce qu'inspirée des modèles actuels, est surtout axée sur la maîtrise des risques et moins sur la maîtrise des coûts. Ce document ne propose pas une réelle approche de type "coût / bénéfice", ce type d'approche pouvant par ailleurs s'avérer difficile à mettre en œuvre. En effet, dans les premiers stades de la conception d'une nouvelle centrale, les coûts de construction mais surtout d'exploitation ne sont pas encore bien connus. Il est alors difficile de chiffrer tel ou tel ensemble de solutions. L'approche proposée a cela de robuste qu'elle ne nécessite que l'estimation (de toute façon indispensable) de l'impact sur le risque de chaque élément.

[6]Une EPS de niveau 2 aurait pu valoriser un tel apport.

Conclusion générale

L'objectif de cette thèse était d'identifier et de réduire les incertitudes sur les mesures d'importance issues des EPS, puis de proposer de nouvelles applications utilisant ce type d'indicateurs. Le contexte industriel de cette thèse imposait de plus de travailler à "modèle EPS constant", c'est-à-dire sans trop modifier les modèles EPS et en conservant le même logiciel support (Risk Spectrum).

Les mesures d'importance issues des EPS sont utilisées dans des applications ayant un impact sur la sûreté. On doit donc contrôler les incertitudes portant sur ces indicateurs et les réduire dans la mesure du possible. En effet, la réduction de ces incertitudes ne doit pas impliquer de trop grosses modifications des modèles EPS d'EDF, ni une trop grosse charge de travail pour les ingénieurs en charge du calcul et de l'utilisation de ces indicateurs.

Ces mesures d'importance peuvent être affectées par des incertitudes stochastiques et par des incertitudes épistémiques [71]. Les incertitudes stochastiques sont dues au caractère intrinsèquement aléatoire des phénomènes observés, alors que les incertitudes épistémiques sont dues aux simplifications faites dans les modèles et dans les logiciels supportant ces modèles.

Après avoir pris connaissance des nombreux travaux portant sur les incertitudes stochastiques, nous avons conclu que le cadre théorique permettant la prise en compte de telles incertitudes était déjà bien établi même si sa mise en œuvre se heurte au manque de données permettant de caractériser le comportement aléatoire des différents phénomènes que l'on cherche à modéliser. Nous avons donc fait le choix de ne pas travailler sur ce type d'incertitudes.

Les incertitudes épistémiques peuvent être inhérentes au type de modélisation choisi. Ainsi, les modèles booléens qui servent de cadre au développement des EPS d'EDF ne permettent pas de considérer l'ordre d'occurrence des événements, alors que cet ordre peut avoir un impact sur la dynamique de l'accident. Dans la mesure où les choix de modélisation ne devaient pas être remis en cause, les simplifications imposées par l'utilisation des modèles booléens n'ont pas été étudiées. Cependant, les incertitudes épistémiques peuvent aussi être dues aux simplifications faites lors de la modélisation, ainsi qu'au logiciel support permettant de mettre en œuvre ces modèles. Ce sont celles-ci qui ont été étudiées dans le cadre de la présente thèse. Ainsi, il est apparu que de nombreuses simplifications faites dans les modèles EPS d'EDF et dans leur logiciel support ne généraient que peu d'incertitudes sur le risque de référence (probabilité d'occurence de l'événement CI), mais posaient problème lorsque ces modèles étaient utilisés pour déterminer l'importance d'événements autres que l'événement CI (CI correspond à l'événement "fusion du cœur" pour les EPS de niveau 1 et à l'événement "rejets précoces et massifs" pour les EPS de niveau 2). Pour pallier à ces déficiences, nous avons défini des recommandations en termes de modélisation et développé un nouveau processus de troncation du jeu de coupes de référence qui permet un calcul rapide et précis des mesures d'importance. Cette démarche de troncation à été mise en œuvre au sein d'un prototype de logiciel de post-traitement des résultats de RSW (SENSIB) pour pouvoir calculer plus précisément, plus rapidement et de

manière automatique les mesures d'importance issues des EPS. Cette application permet de plus de bien mieux informer l'utilisateur sur leurs incertitudes.

Une fois les modèles EPS capables de calculer des différentes mesures d'importance, de nouvelles applications utilisant ce type d'indicateurs peuvent être développées. Pour ce faire, nous avons cherché à définir quels indicateurs pouvaient être utiles pour quelles applications.

Dans un premier temps, il nous a semblé opportun d'étendre la définition des mesures d'importance les plus connues, de manière à pouvoir considérer en plus des événements élémentaires (les EB) des macro-événements tels que la défaillance d'un système, la non-existence d'une fonction ou la perte simultanée de matériels liés par des critères "Géographiques Technologiques ou Physiques" (les critères PGT). Ces facteurs d'importance "étendus" aux macro-événements ont trouvé leur première application dans le cadre de l'étude portant sur la redéfinition des délais de repli (les délais avant l'arrêt de la centrale) en cas de cumuls d'indisponibilités de matériels importants pour la sûreté. Nous avons ainsi proposé deux indicateurs permettant d'estimer l'augmentation de la contribution au risque et de la contribution à la sûreté des autres matériels importants pour la sûreté, lorsque deux d'entre eux sont défaillants.

Dans un second temps, l'utilisation de mesures d'importance pour aider à la conception de nouvelles centrales nucléaires à été envisagée. Ainsi, nous avons défini une ébauche de ce que pourrait être une démarche de conception utilisant conjointement une approche probabiliste et une approche déterministe. Cette démarche se décompose en quatre étapes. La première consiste à définir le fonctionnement général de la centrale de manière déterministe. Les méthodes et outils utilisés durant cette première étape n'ont pas fait l'objet de notre étude. La deuxième étape consiste tout d'abord à modéliser ce fonctionnement dans une EPS simplifiée, appelé EPS "compacte". Une fois ce modèle construit, nous avons proposé des méthodes qui permettent d'aider à la définition et à la répartition des lignes de défense au moyen de mesures d'importance classiques, telles que le Facteur d'Accroissement de Risque (FAR) ou le Facteur de Diminution de Risque (FDR). La troisième étape consiste à concevoir le fonctionnement de chacune de ces lignes de défense au moyen d'une approche déterministe, qui repose sur des méthodes déjà bien établies lors de la conception des générations de centrales existantes. Durant la dernière étape, on modélise le fonctionnement détaillé de la centrale dans une EPS complète. Au moyen de ce modèle "complet", nous avons proposé, à l'aide de nouvelles mesures d'importance, une démarche d'identification des interdépendances qui posent problème en termes de défense en profondeur, ainsi que de celles dont l'existence contribue à augmenter la valeur du risque. De plus, nous avons proposé d'autres indicateurs permettant d'identifier les modifications de conception nécessaires pour réduire ces interdépendances.

Il pourrait être intéressant d'enrichir cette démarche de conception en essayant d'y intégrer les coûts de construction et d'exploitation respectifs des différentes solutions envisagées. De même, les méthodes de modélisation qui permettraient d'intégrer au sein des EPS les actions de surveillance et de maintenance restent à définir. Grâce à une telle prise en compte, il deviendrait possible de valoriser leur impact bénéfique sur le risque et, lors de la conception, de mieux répartir les ressources entre les lignes de défense (matérielles ou organisationnelles) prévenant l'accident et celles en réduisant l'impact.

De même, si on connaît maintenant mieux l'impact de la troncation du jeu de coupes en termes d'incertitude sur les mesures d'importance, nous n'avons pas quantifié celui des simplifications de modélisation. Une telle estimation serait pourtant utile pour hiérarchiser les modifications à apporter aux modèles EPS avant tout calcul de mesures d'importance.

On peut enfin noter que les modes de calcul des mesures d'importance étendues que nous avons proposés sont encore très manuels. Leur automatisation et leur intégration au sein de

l'application SENSIB pourrait être le moyen d'en promouvoir le développement en réduisant leur coût de mise en œuvre.

D'autres questions d'ordre plus général restent ouvertes. Ainsi, cette thèse a mis à jour de nombreuses limites de RSW. Si l'impératif de travailler à modèle constant était levé, on pourrait envisager d'utiliser d'autres types de modélisation qui permettraient de prendre en compte plus finement le comportement des centrales. Ainsi, si la prise en compte de processus dynamiques dans les EPS ne semble pas encore d'actualité, il pourrait être intéressant de lever l'hypothèse de cohérence du fonctionnement d'une centrale ou de supprimer l'obligation de tronquer la fonction de structure modélisant celui-ci. De plus, d'autres logiciels supports pourraient sans doute permettre un calcul plus aisé des différentes mesures d'importance et on pourrait alors se passer de l'utilisation de logiciels de post-traitement.

Par ailleurs, les limites propres à la nature des mesures d'importance n'ont pas toutes été levées. Elles ne permettent par exemple pas de prendre en compte l'impact, en termes de risque, de plusieurs décisions basées sur leur utilisation. Or, le cumul de plusieurs décisions qui, prises isolément, ont chacune un impact bénéfique sur le risque, pourrait conduire à une diminution du niveau de sûreté [49]. Ainsi, lors de la mise en œuvre de démarches basées sur des mesures d'importance, on est contraint de modéliser chaque modification avant de pouvoir en envisager une autre.

En outre, les mesures d'importance sont relatives au type de risque considéré [49]. On pourrait imaginer des métriques de risque autres que le risque de fusion du cœur. On pourrait ainsi considérer des risques financiers ou des risques en termes de santé publique. L'importance de chaque événement n'est donc pas une valeur intrinsèque, mais elle est relative aux autres événements et au risque considéré. Ainsi, l'enceinte de confinement n'est pas importante lorsqu'on considère le risque de fusion du cœur, mais elle le devient lorsqu'on considère les risques de rejet de matériaux radioactifs dans l'environnement. Une métrique pertinente permettant de comparer tous les événements relatifs au fonctionnement d'une centrale, ainsi que les incertitudes auxquelles elle pourrait être soumise, reste largement à définir.

Bibliographie

[1] AEN/OCDE. Méthode d'évaluation des conséquences économiques des accidents nucléaires. Rapport d'étude, Agence pour l'énergie nucléaire, 2000.

[2] AFCEN. Règles de conception et de construction applicables aux assemblages de combustible des centrales nucléaires. Technical Report RCC-C, Association Française des Constructeurs de l'Énergie Nucléaire, 1984. modificatifs : juillet 86, sept.89, déc.93 et sept.95.

[3] AFCEN. Règles de conception et de construction applicables aux matériels mécaniques des ilôts nucléaires. Technical Report RCC-M, Association Française des Constructeurs de l'Énergie Nucléaire, juin 2000. modificatifs : juin 2002, décembre 2005.

[4] AFCEN. Règles de conception et de construction applicables aux matériels électriques des ilôts nucléaires. Technical Report RCC-E, Association Française des Constructeurs de l'Énergie Nucléaire, décembre 2005. modificatifs : juillet 86, sept.89, déc.93 et sept.95.

[5] AIEA. Basic safety principles for nuclear power plants. Rapport 75-INSAG-3 rev. 1/a, Agence Internationale de l'Énergie Atomique (AIEA), Vienne Autriche, 1999.

[6] AIEA. Considerations in the development of safety requirements for innovative reactors : Application to modular high temperature gas cooled reactors. Technical Report IAEA-TECDOC-1366, Agence Internationale de l'Énergie Atomique (AIEA), Vienna Austria, 2003.

[7] C. Ancelin, M. Bouissou, J. Collet, M. Gallois, L. Magne, N. Villate, C. Yedid, et D. Mulet-Marquis. From LESSEPS to the workstation for reliability engineers. *Reliability Engineering & System Safety*, 44(3) :313–323, 1994.

[8] G. Apostolakis et P. Moieni. The foundations of models of dependence in probabilistic safety assessment. *Reliability Engineering & System Safety*, 18 :177–195, 1987.

[9] M. Balmain. Accélération de calculs dans les EPS et ajustement des seuils de coupe. note technique HT-51/06/003/A, EDF, 2006.

[10] S. Beeson et J. Andrews. Calculating the failure intensity of a non-coherent fault tree using the BDD technique. *Quality and reliability engineering international*, 20 :225–235, 2004.

[11] Z. W. Birnbaum. On the importance of different components in a multicomponent system. Technical Report AD0670563, Washington University of Seattle laboratory of statistical research, 1968.

[12] P. J. Boland et E. El-Neweihi. Measures of component importance in reliability theory. *Computers and Operations Research*, 4 :455–463, 1995.

[13] E. Borgonovo. Differential, criticality and Birnbaum importance measures : An application to basic event, groups and SSCs in event trees and binary decision diagrams. *Reliability Engineering & System Safety*, In press, 2006.

[14] E. Borgonovo, G. E. Apostolakis, S. Tarantola, et A. Saltelli. Comparison of global sensitivity analysis techniques and importance measure in PSA. *Reliability Engineering & System Safety*, 79 :175–185, 2003.

[15] M. Bouissou. Gestion de la complexité dans les études quantitatives de sûreté de fonctionnement des systèmes. Habilitation à diriger des recherches, Université des Sciences et Technologies de Lille (USTL), 2007.

[16] M. Bouissou, F. Bruyère, C. Belly, et T. Hutinet. Comparaison de méthodes de traitement de fonctions booléennes. note technique HT-52/97/038A, EDF R&D, Clamart, France, 1997.

[17] M. Bouissou, F. Bruyere, et A. Rauzy. BDD based fault-tree processing : a comparison of variable ordering heuristics. In C. G. Soares, editor, *Advancend in Safety and Reliability ESREL'97*, pages 2045–2051, Lisbonne, Portugal, Juin 1997. ESRA, Pergamon.

[18] G. Bourgeois, Y. Driencourt, et I. Renault. Les facteurs d'importance. note technique HT-53/97/027/A, EDF R & D, 1998.

[19] M. Čepin. Analysis of truncation limit in probabilistic safety assessment. *Reliability Engineering & System Safety*, 87 :395–403, 2005.

[20] M. C. Cheok, G. W. Parry, et R. R. Sherry. Use of importance measures in risk-informed regulatory applications. *Reliability Engineering & System Safety*, 60 :213–226, 1997.

[21] E. Châtelet, Y. Dutuit, A. Rauzy, et T. Bouhoufani. An optimization procedure to generate sums of disjoint products. *Reliability Engineering & System Safety*, 65 :289–294, 1999.

[22] S. Combacon, Y. Dutuit, A. Laviron, et A. Rauzy. Comparison between two tools (Aralia and ESCAF) applied to the study of the emergency shutdown system of a nuclear reactor. In A. M. et R.A. Bari, editor, *Fourth congress on Probabilistic Safety Assessment and Management (PSAM04)*, pages 1019–1024, New York, USA, Septembre 1998. IAPSAM, Springer.

[23] Comité RCC. Rcc applicables aux procédés du palier 1400 mwe n4. Technical Report RCC-P, Association Française des Constructeurs de l'Énergie Nucléaire, octobre 1991.

[24] Comité RCC. Rcc applicables à la protection contre l'incendie. Technical Report RCC-I, Association Française des Constructeurs de l'Énergie Nucléaire, octobre 1997.

[25] A.-S. Derode. *Approximation de la fiabilité : cas des systèmes à réparation différées ou à composants viellissants*. PhD thesis, Université de Lille 1 (USTL), 2007.

[26] J. Dewailly. Guide méthodologique d'estimation des paramètres de DCC pour les groupes de matériels redondants de taille inférieure à quatre. note technique HT-51-/05/024/04, EDF R&D, 2005.

[27] J. Dewailly et A. Dubreuil-Chambardel. Utilisation des EPS pour optimiser la maintenance des REP en france : quelques tendances de la recherche. note technique HT-51/94/012A, EDF R&D, Clamart, France, 1994.

[28] L. Dieulle, A. Grall, C. Bérenguer, et A. Barros. Modèles de défaillances de cause commune, REX et estimation de paramètres, 2004. Rapport final de contrat d'association EDF/R&D/UTT- Contrat T51/G27369.

[29] A. Dubreuil-Chambardel. Proposal to select critical equipments in a RCM project and links with the definition of maintenance task. note technique HT-50/94/008B, EDF R&D, Clamart, France, 1995.

[30] N. Duflot. How to control the uncertainty of importance measures in PSA : EDF good practices. note interne technique NIT-T51/06/01, EDF R&D, 2006.

[31] N. Duflot, C. Bérenguer, L. Dieulle, et D. Vasseur. Calculating importance measures in PSA at different levels. In G. S. et E. Zio, editor, *Safety and Reliability for Managing Risk*, pages 2405–2412, Estoril, Portugal, Septembre 2006. ESRA, Taylor & Francis.

[32] N. Duflot, C. Bérenguer, L. Dieulle, et D. Vasseur. How to build an adequate set of minimal cut sets for PSA importance measure calculation. In M. Stamatelatos et H. Blackman, editors, *Eighth congress on Probabilistic Safety Assessment and Management (PSAM08)*, Nouvelle Orléans, USA, Mai 2006. IAPSAM, ASME Press. papier 71.

[33] N. Duflot, C. Bérenguer, L. Dieulle, et D. Vasseur. On the independence of defense lines of a new nuclear power plant. In *ESREL'07*. ESRA, 2007. papier 242.

[34] N. J. Duijm, H. B. Andersen, A. Hale, L. Gossens, et D. Hourtolou. Evaluating and managing safety barriers in major hazard plants. In U. S. C. Spitze et V. Dang, editors, *Probabilistic Safety Assessment and Management (PSAM07 & ESREL'04)*, pages 110–115, Berlin, Allemagne, Juin 2004. IAPSAM & ESRA, Springer.

[35] H. Duncan Brewer et K. S. Canady. Probabilistic safety assesment support for the maintenance rule at Duke Power Company. *Reliability Engineering & System Safety*, 63 :243–249, 1999.

[36] Y. Dutuit et A. Rauzy. Efficient algorithms to assess component and gate importance in fault tree analysis. *Reliability Engineering & System Safety*, 72 :213–222, 2001.

[37] Y. Dutuit et A. Rauzy. Approximate estimation of system reliability via fault trees. *Reliability Engineering & System Safety*, 87 :163–172, 2005.

[38] EDF. Document standard des spécifications techniques d'exploitation du palier CP0. note D4510/EXF/N/97-389, Électricité De France, 1997.

[39] EDF. Mémento de la sûreté nucléaire en exploitation, 2004.

[40] EPRI. PSA applicaton guide. Technical report, EPRI, 1995.

[41] EPRI. Insights from EPRI maintenance rule projects. Technical report, EPRI, 1996.

[42] EPRI. Reliability and risk significance : For maintenance and reliability professionals at nuclear power plants. Technical Report 1007079, EPRI, 2002.

[43] EPRI. Parametric uncertainty impacts on option 2 safety significance categorization. Technical Report 1008905, EPRI, 2003.

[44] S. Epstein et A. Rauzy. Can we trust PRA ? *Reliability Engineering & System Safety*, 88 :195–205, 2005.

[45] S. Epstein et A. Rauzy. Can we trust PRA ? (take two). In *International Topical Meeting on Probabilistic Safety Analysis, PSA'05*, San Francisco, USA, Septembre 2005. American Nuclear Society.

[46] S. Epstein, A. Rauzy, et D. J. Wakefield. Can we trust PRA : take 3. In M. Stamatelatos et H. Blackman, editors, *Eighth congress on Probabilistic Safety Assessment and Management (PSAM08)*, Nouvelle Orleans, USA, Mai 2006. IAPSAM, ASME Press. papier 370.

[47] S. Epstein et D. J. Wakefield. Investigation of binary decision diagram quantification of linked fault trees. Rapport technique CA :2005. 1010062, EPRI, Palo Alto, 2005.

[48] ERIN Engineering. PRA quantification truncation and convergence guide. (draft report), EPRI, Palo Alto, 2004.

[49] K. Fleming. Issues and Recommendations for A dvancement of PRA Technology in Risk-Informed Decision Making. Technical Report NUREG/CR-6813, U.S. Nuclear Regulatory Commission, 2003.

[50] K. N. Fleming et F. A. Silady. A risk informed defense-in-depth framework for existing and advanced reactors. *Reliability Engineering & System Safety*, 78 :205–225, 2002.

[51] M. V. Frank et K. N. Fleming. Risk-significant functional dependencies in pressurized water reactors. *Reliability Engineering & System Safety*, 34 :293–308, 1991.

[52] M. Gallois. Guide de réalisation des études de séquences pour les EPS de référence. note technique HT-51/03/003/A, EDF R& D, 2003.

[53] M. Gallois. Prise en compte du facteur humain dans les EPS de référence. note technique HT-51/01/014A, EDF R&D, 2003.

[54] M. Gallois et M. Villermain. Bilan comparatif des EPS de référence. note technique HT-51/01/026/A, EDF R&D, 2002.

[55] Groupe Consultatif Français de Sûreté. Safety objectives, approach and methods for the design and the assessment of future nuclear systems. Nice, France, Mai 2007. Société Française D'Énergie Nucléaire. papier 7168.

[56] P. J. Haas. *Stochastic Petri nets*. Springer, 2002.

[57] A. Hale, L. Goossens, B. Ale, L. Bellamy, J. Post, J. Oh, et I. A. Papazoglou. Managing safety barriers and controls at the workplace. In U. S. C. Spitze et V. Dang, editors, *Probabilistic Safety Assessment and Management (PSAM07 & ESREL'04)*, pages 608–613, Berlin, Germany, Juin 2004. IAPSAM & ESRA, Springer.

[58] K. D. Heidtmann. Smaller sums of disjoint products by subproduct inversion. *IEEE Transactions on Reliability*, 38 :305–311, 1989.

[59] J. C. Helton et F. J. Davis. Latin hypercube sampling and the propagation of uncertainty of complex systems. *Reliability Engineering & System Safety*, 81 :23–69, 2003.

[60] E. Hollnagel. Accidents and barriers. In *European conference on cognitive science approaches to process control*, pages 175–180, France, 1993.

[61] L. Jacobson Kecklund, A. Edland, P. Wedin, et O. Svenson. Safety barrier function analysis in a process industry : a nuclear power application. *International journal of industrial ergonomics*, 17 :275–284, 1996.

[62] W. S. Jung, J. E. Yang, et J. Ha. Development of measures to estimate truncation error in fault tree analysis. *Reliability Engineering & System Safety*, 90 :30–36, 2005.

[63] M. Llory. Les facteurs d'importance dans les EPS. Synthèse bibliographique ITH-95-R14, Institut de travail humain, 2006.

[64] S. Martorell, V. Serradell, et G. Verdú. Safety-related equipment prioritization for reliability centered maintenance purposes based on a plant specific level 1 PSA. *Reliability Engineering & System Safety*, 52 :35–44, 1995.

[65] F. C. Meng. Some further results on ranking the importance of system components. *Reliability Engineering & System Safety*, 47 :97–101, 1995.

[66] F. C. Meng. Relationship of Fussell-Vesely and Birnbaum importance to structural importance in coherent systems. *Reliability Engineering & System Safety*, 67 :55–60, 1999.

[67] M. Modarres et H. Dezfuli. A truncation methodology for evaluating large fault trees. *IEEE Transactions on Reliability*, 33(4) :325–328, 1984.

[68] F. Moneron Dupin. Méthode pratique de prise en compte du facteur humain dans les études de séquences accidentelles. note technique EPS FH 007 A, EDF DER - ESF, 1989.

[69] A. Mosleh, K. Fleming, G. W. Parry, H. M. Paula, D. H. Worledge, et D. M. Rasmuson. Procedures for treating Common Cause Failures in safety and reliability studies - analytical background and techniques. Technical Report NUREG/CR-4780 - EPRI/NP5613 - Volume 2, U.S. Nuclear Regulatory Commission, 1989.

[70] M. Nikolskaia et A. Rauzy. Application des diagrammes binaires d'expression au traitement d'arbres de défaillance. In 12e *Colloque National de Sûreté de Fonctionnement (λ μ 12)*, Montpellier, France, Mars 2000. IMDR.

[71] A. O'Hagan et J. E. Oakley. Probability is perfect, but we can't elicit it perfectly. *Reliability Engineering & System Safety*, 85 :239–248, 2004.

[72] B. Papin et P. Quellien. The operational complexity index : a new method for the global assessment of the human factor impact on the safety of advanced reactors concepts. *Nuclear engineering and design*, 236 :113–1121, 2006.

[73] H. Pesme et P. Meyer. Guide d'application de la méthode MERMOS d'évaluation probabiliste de la fiabilité humaine pour les EPS de référence. note technique HT 54/02/020, EDF R&D, 2002.

[74] A. Rauzy. New algorithms for fault trees analysis. *Reliability Engineering & System Safety*, 40 :203–211, 1993.

[75] A. Rauzy. A brief introduction to binary decision diagrams. *RAIRO-APII-JESA, Journal européen des systèmes automatisés*, 30 :1033–1051, 1996.

[76] A. Rauzy, E. Chatelet, Y. Dutuit, et C. Bérenguer. A practical comparison of methods to assess sum-of-products. *Reliability Engineering & System Safety*, 79 :33–42, 2003.

[77] J. M. Reinert et G. E. Apostolakis. Including model uncertainty in risk-informed decision making. *Annals of nuclear energy*, 33 :354–369, 2006.

[78] RELCON. Risk spectrum theory manual. manuel d'utilisation, RELCON, 2004.

[79] F. Rossignol et S. Vidal. Simplification utilisées dans les EPS de niveau 1. note technique HT-51/02/008/A, EDF R&D, Clamart, France, 2002.

[80] S. Sklet. Safety barriers : definition, classification, and performance. *Journal of loss of prevention in the process industries*, 19 :494–506, 2005.

[81] J. Sorensen, G. Apostolakis, T. Kress, et D. Powers. On the role of defense in depth in risk informed regulation. In *International Topical Meeting on Probabilistic Safety Analysis, PSA'99*, pages 22–25, Washington DC, USA, 1999. American Nuclear Society.

[82] A. D. Swain. Accident sequence evaluation program human reliability analysis procedure. Technical Report NUREG/CR 4772, Nuclear Regulatoy Commission, 1987.

[83] US Nuclear Regulatory Comission. Individual plant examination program : perspectives on reactor safety and plant performance. Final report NUREG-1560, USNRC, 1997.

[84] M. Van Der Borst et H. Schoonakker. An overview of PSA importance measures. *Reliability Engineering & System Safety*, 72 :241–245, 2001.

[85] D. Vasseur. Méthode EPS de gestion des cumuls d'indisponibilité appliquée aux conditions limites et première application. Technical Report H-T51-2006-01690-FR, EDF R&D, 2006. note technique.

[86] D. Vasseur et B. Lapirot. Impact des DCC sur les programmes de maintenance établis dans le cadre de l'OMF. note technique HT-51/03/024/A, EDF R & D, 2003.

[87] D. Vasseur, A. Voicu, C. Bérenguer, et A. Grall. Importance factors and common cause failure : wich impact on preventive maintenance program optimization ? In *International Topical Meeting on Probabilistic Safety Analysis, PSA'05*, San Francisco, USA, Septembre 2005. American Nuclear Society.

[88] J. K. Vaurio. Configuration management and maintenance ranking by reliability importance measures. In G. S. . E. Zio, editor, *Safety and Reliability for Managing Risk*, Estoril, Portugal, Septembre 2006. ESRA, 633–641.

[89] J. K. Vaurio. Developments in importance measures for risk-informed ranking and other applications. In M. Stamatelatos et H. Blackman, editors, *Eighth congress on Probabilistic Safety Assessment and Management (PSAM08)*, Nouvelle Orleans, USA, Juin 2006. IAPSAM, ASME Press. papier 46.

[90] W. Vesely et G. Apostolakis. Editorial : Dévelopments in risk-informed decision-making for nuclear power plants. *Reliability Engineering & System Safety*, 63 :223–224, 1999.

[91] W. E. Vesely. The use of risk importances for risk-based applications and risk-based regulations. In *International Topical Meeting on Probabilistic Safety Assessment (PSA96)*, pages 1623–1631, Park City, Utha, USA, Sept.-Oct. 1996. American Nuclear Society.

[92] W. E. Vesely. Reservations on "ASME risk-based inservice inspection and testing : an outlook to the future". *Risk analysis*, 18 :423–425, 1998.

[93] W. E. Vesely. Supplemental viewpoints on the use of importance measures in risk-informed regulatory applications. *Reliability Engineering & System Safety*, 60 :257–259, 1998.

[94] W. E. Vesely, M. Belhadj, et J. T. Rezos. PRA importance measures for maintenance prioritization applications. *Reliability Engineering & System Safety*, 43 :307–318, 1994.

[95] W. E. Vesely et T. C. Davis. Evaluations and utilizations of risk importances. Technical Report NUREG/CR-4377, Battelle's columbus laboratories, 1985.

[96] A. Villemeur. *Sûreté de fonctionnement des systèmes industriels.* Collection de la direction des études et recherches d'électricité de France. Eyrolles, 1988.

[97] J. E. Vinnem, T. Aven, S. Hauge, J. Seljelid, et G. Veire. Integrated barrier analysis in operational risk assessment in offshore petroleum operations. In U. S. C. Spitze et V. Dang, editors, *Probabilistic Safety Assessment and Management (PSAM07 & ESREL'04)*, pages 620–625, Berlin, Allemagne, Juin 2004. IAPSAM & ESRA, Springer.

[98] I. B. Wall, J. J. Haugh, et D. H. Worlege. Recent applications of PSA for managing nuclear power plant safety. *Reliability Engineering & System Safety*, 39 :367–425, 2001.

[99] I. B. Wall et D. H. Worledge. Some perspectives in importance measures. In *International Topical Meeting on Probabilistic Safety Assessment*, pages 203–207, Park City, USA, Sept-Oct 1996. American Nuclear Society.

[100] R. Youngblood. Risk significance and safety significance. *Reliability Engineering & System Safety*, 73 :121–136, May 2001.

Index

Annexe A

Modèles de l'application numérique de la section 1.7 du chapitre 1

Cette annexe présente les arbres de défaillances et les données de fiabilité utilisées pour supporter l'exemple d'application numérique du calcul des facteurs d'importance à différents niveaux présenté dans la section 1.7 du chapitre 1.

La modélisation de la défaillance des pompes 1 et 2 du schéma de la figure 3.1 est présentée dans la figure A.1.

La défaillance de l'injection aux joints de pompes primaires (IJPP) est modélisée au moyen de l'arbre de défaillances de la figure A.2.

La défaillance de la ligne de charge (ILC) est modélisée au moyen de l'arbre de défaillances de la figure A.3.

La défaillance de l'injection de sécurité haute pression (ISHP) est modélisée au moyen de l'arbre de défaillances de la figure A.4.

La défaillance de l'alimentation de secours des générateurs de valeurs (ASG) est modélisée au moyen de l'arbre de défaillances de la figure A.5.

La défaillance de l'injection de sécurité basse pression (ISBP) est modélisée au moyen de l'arbre de défaillances de la figure A.6.

Les probabilités d'occurrence de chacun des événements de base modélisés dans ces arbres de défaillances se trouve dans le tableau A.1.

EB	probabilité	*EB*	probabilité	*EB*	probabilité
`P1_D`	10^{-3}	`V21_F`	10^{-3}	`V_2F`	10^{-3}
`P2_D`	10^{-3}	`V22_F`	10^{-3}	`ASG_int_D`	10^{-4}
`P1_M`	10^{-3}	`V11_F`	10^{-3}	`ASG_VP_D`	10^{-2}
`P2_M`	10^{-3}	`V12_F`	10^{-3}	`ISBP_int_D`	10^{-4}
`El`	10^{-10}	`V1_F`	10^{-3}		

Tab. A.1 – *Probabilité d'occurrence de chaque événement de base de l'application numérique*

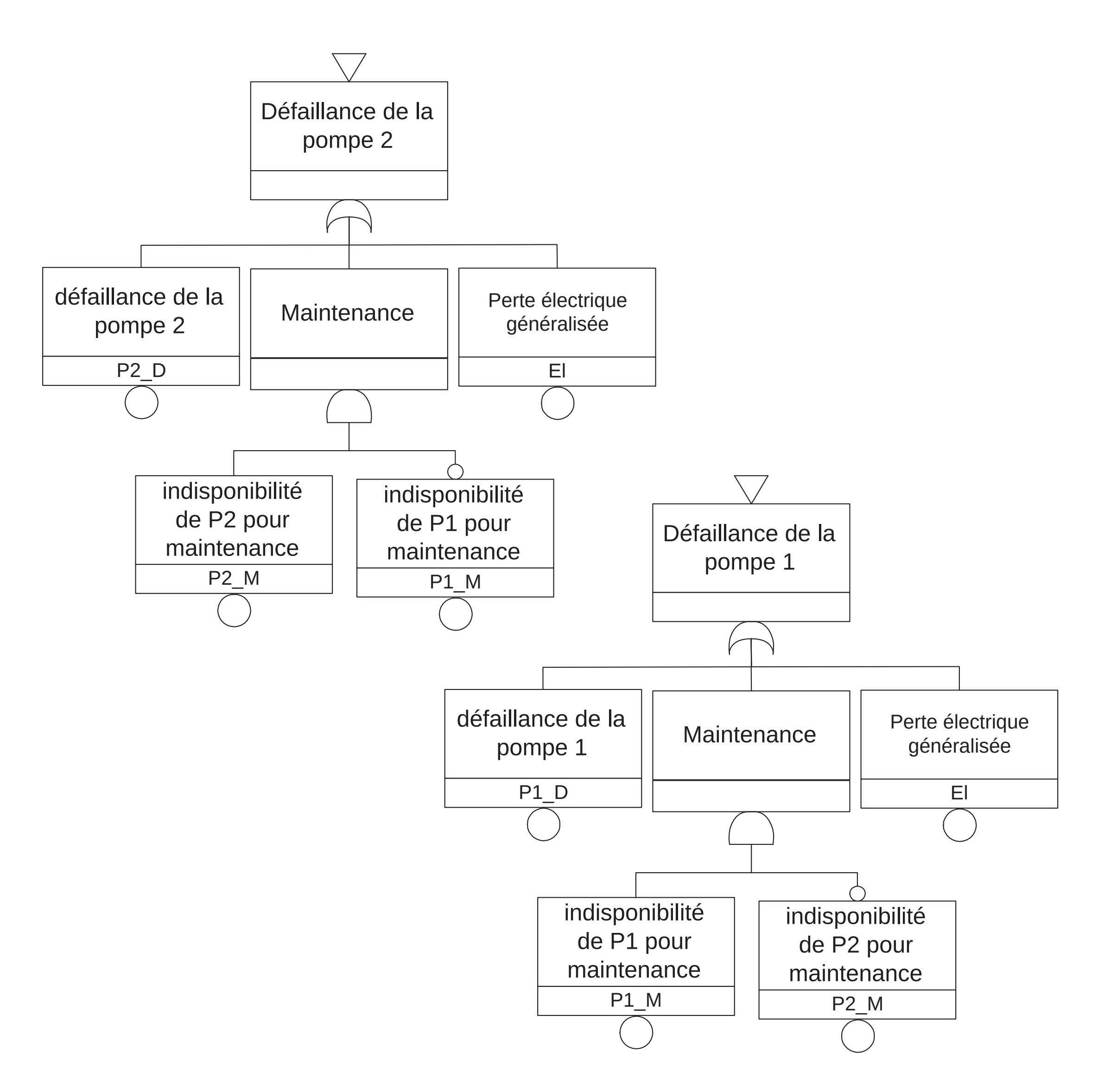


FIG. A.1 – *Modélisation des défaillances des pompes 1 et 2*

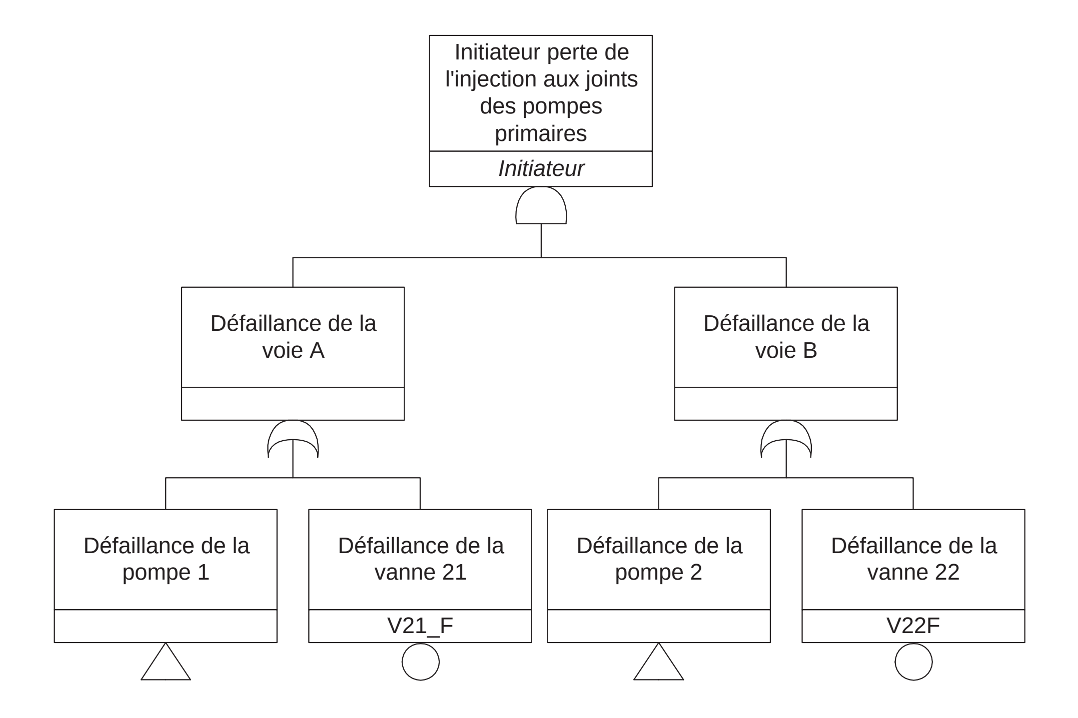


FIG. A.2 – *Modélisation de l'initiateur "défaillance de l'injection aux joints des pompes primaires"*

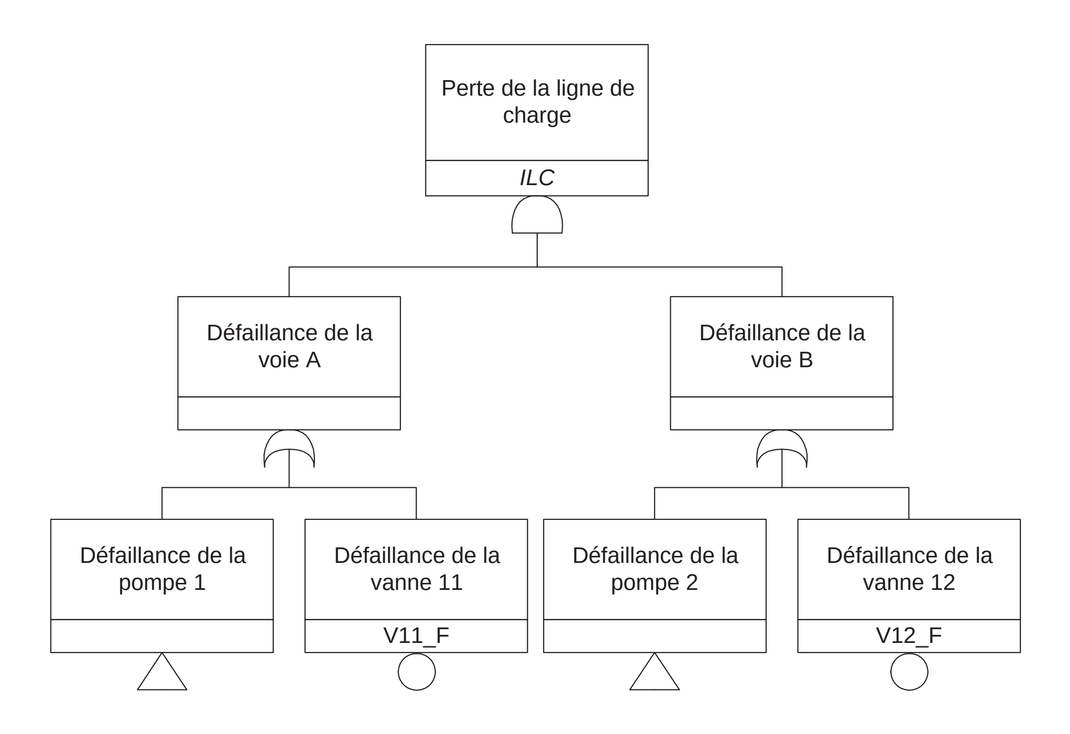


FIG. A.3 – *Modélisation de la défaillance de la ligne de charge*

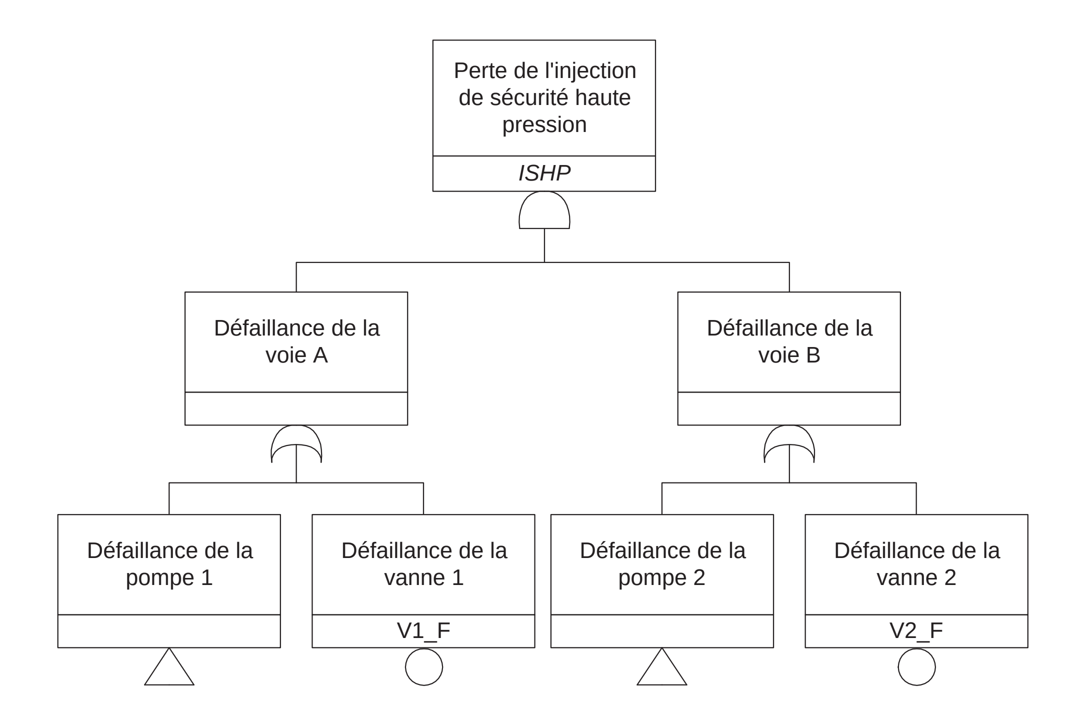


Fig. A.4 – *Modélisation de la défaillance de l'injection de sécurité haute pression*

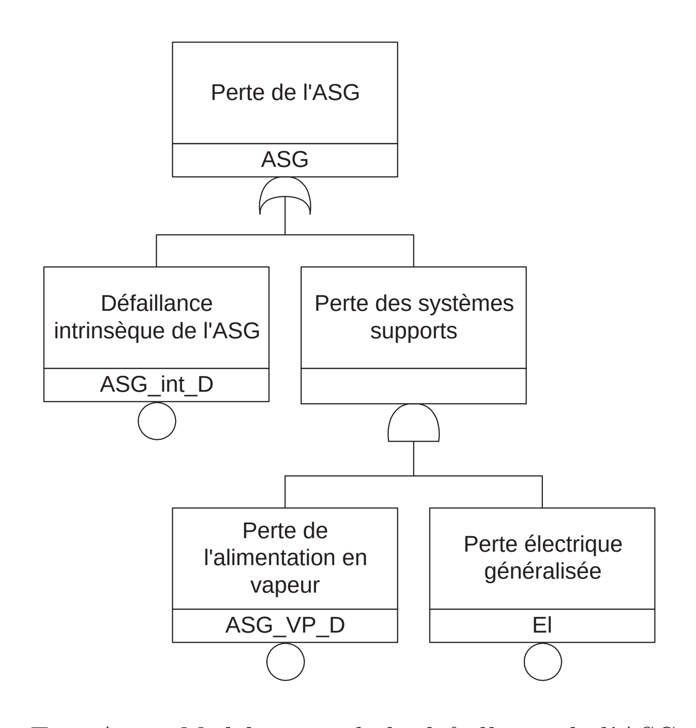


Fig. A.5 – *Modélisation de la défaillance de l'ASG*

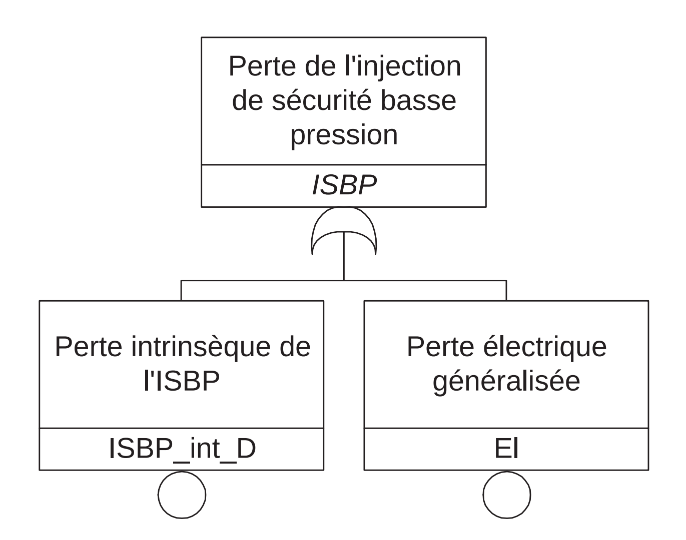


Fig. A.6 – *Modélisation de la défaillance de l'ISBP*

Annexe B

Évolution de la somme des $R_{1,i}$ en fonction du seuil de troncature

L'objectif de cette annexe est de présenter l'évolution de la somme des $R_{1,i}$ calculés à partir du jeu de coupes de référence en fonction de la valeur du seuil de troncature appliqué lors de la génération de ce jeu de coupes. Les figure B.1, B.2 et B.3 présentent ces résultats.

Pour obtenir ces courbes, la somme des $R_{1,i}$ est approximée par :

$$f\left(seuil\right) = \sum_{\substack{EB_i \\ Q(EB_i) \geq 10^{-10}}} \left(\sum_{Q(Coupe_j) \geq seuil} Q\left(Coupe_j / EB_i\right) \right)$$

En observant ces figures on voit que pour un seuil inférieur à 10^{-11}, la somme des $R_{1,i}$ est une fonction concave du seuil de troncature.

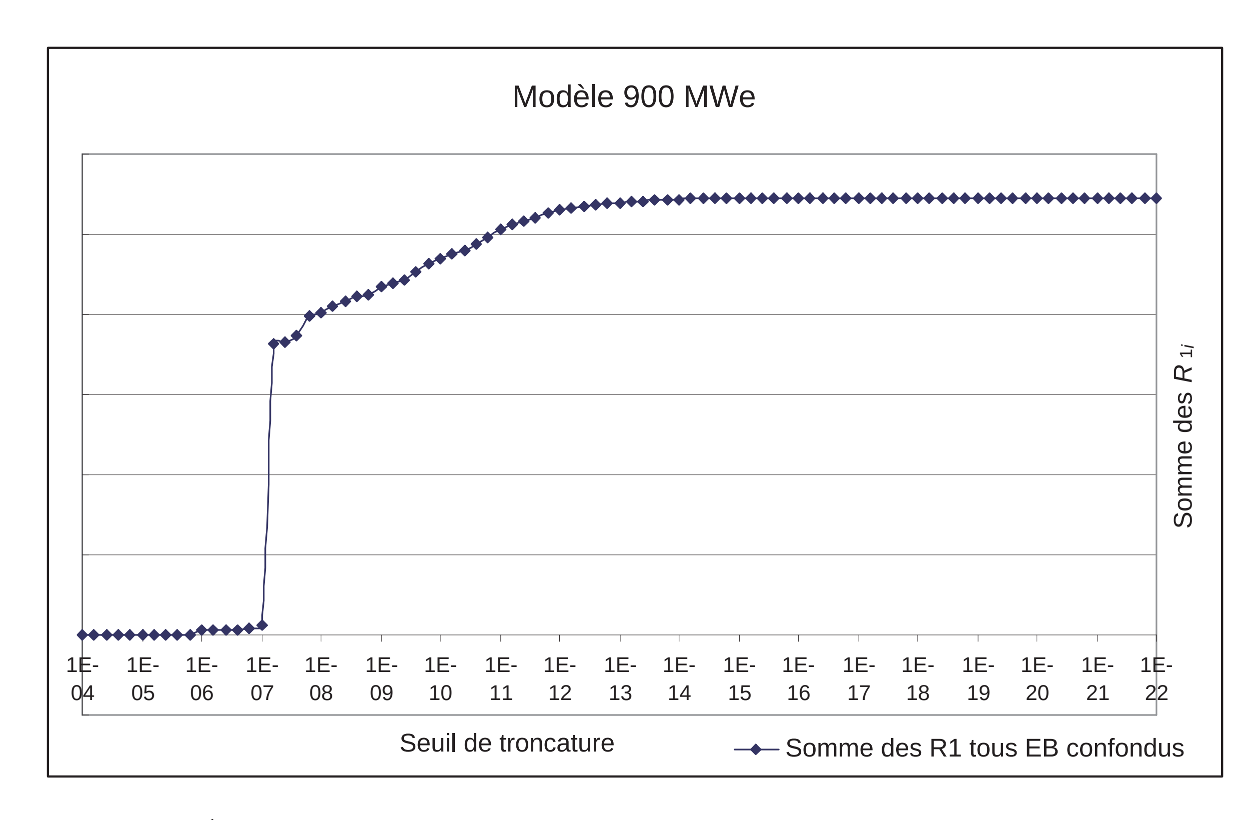


FIG. B.1 – *Évolution de la somme des $R_{1,i}$ en fonction du seuil de troncature des coupes de référence pour le modèle EPS des centrales de 900MWe*

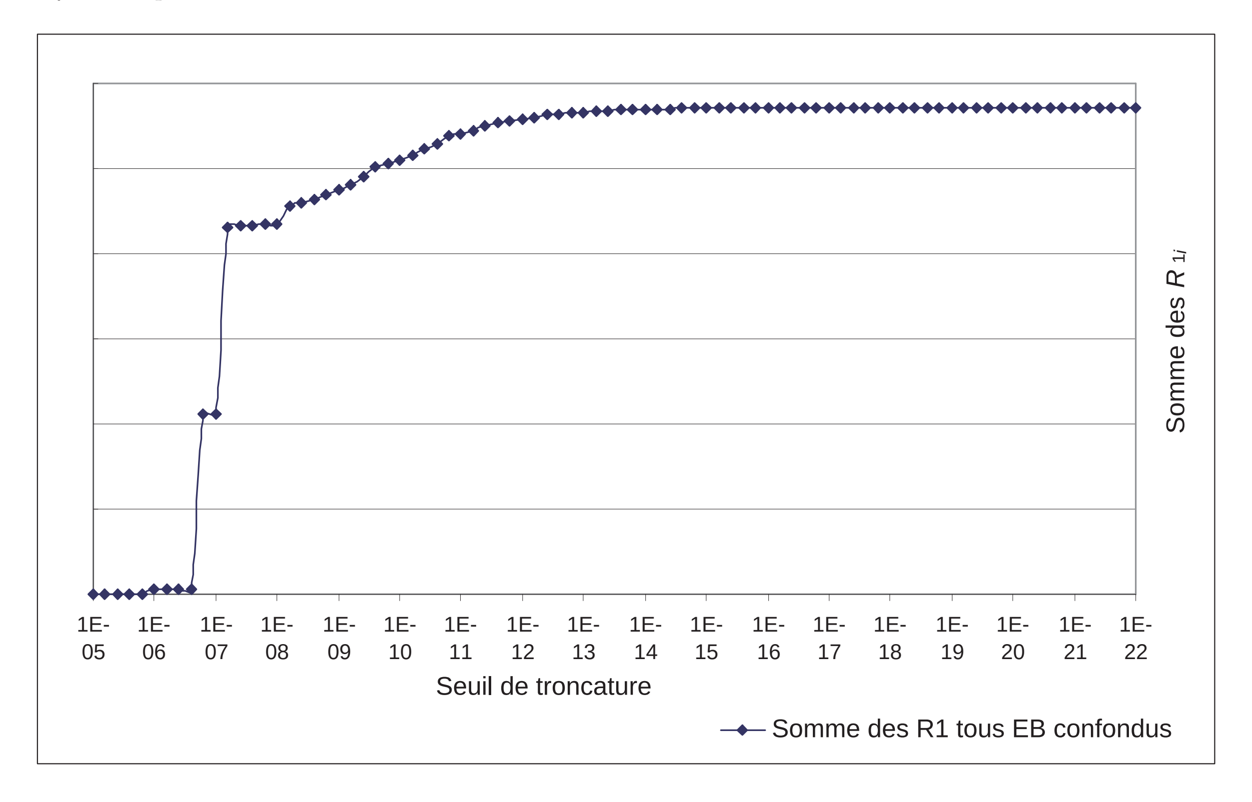


FIG. B.2 – *Évolution de la somme des $R_{1,i}$ en fonction du seuil de troncature des coupes de référence pour le modèle EPS des centrales 1300MWe*

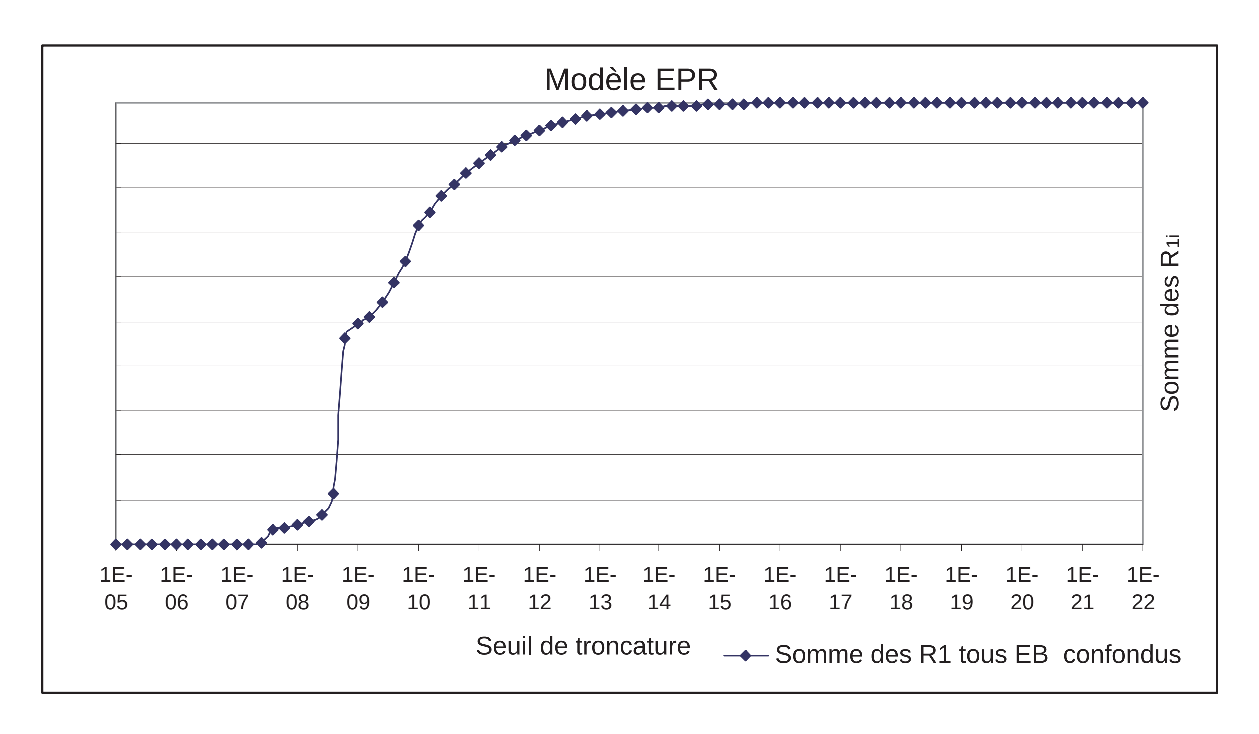


FIG. B.3 – *Évolution de la somme des $R_{1,i}$ en fonction du seuil de troncature des coupes de référence pour le modèle EPS de l'EPR*

Annexe C

Précisions des mesures d'importance calculés avec dix millions de coupes

Pour pouvoir justifier de la nécessité de générer un grand nombre de coupes et donc de les générer initiateur par initiateur, il faut démontrer que les dix millions de coupes que l'on peut générer en une fois ne sont pas suffisantes. Pour ce faire, la valeur de la somme des FAR[1] est tracée en fonction du seuil de troncature utilisé lors de la production des coupes de référence dont ces FAR sont issus.
On voit alors pour le modèle 900PREVD3 que cette somme est sous estimée de près de 30 unités comme nous le montre la figure C.1. Lorsqu'on sait que certaines applications visent à savoir si un FAR est supérieur ou inférieur à 0,05 unité, on voit donc que la précision obtenue avec dix millions de coupes est insuffisante.

Il en va de même avec le modèle EPR comme nous le montre la figure C.2

[1]Cette somme de FAR est obtenue sur le modèle de la somme des $R_{1,i}$ présentée dans la section 2.1.1 du chapitre 2

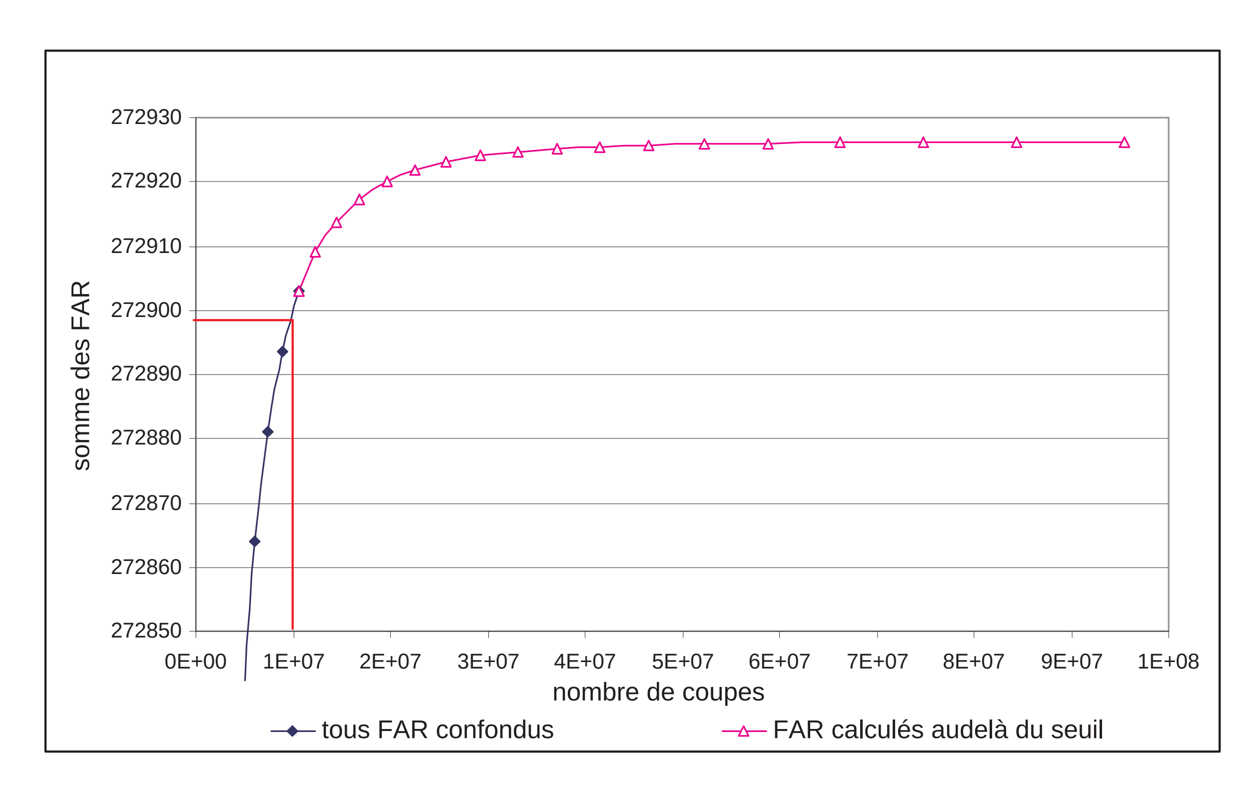


Fig. C.1 – *Valeur de la somme des FAR de tous les EB calculée en fonction du seuil de troncature pour le modèle 900PREVD3*

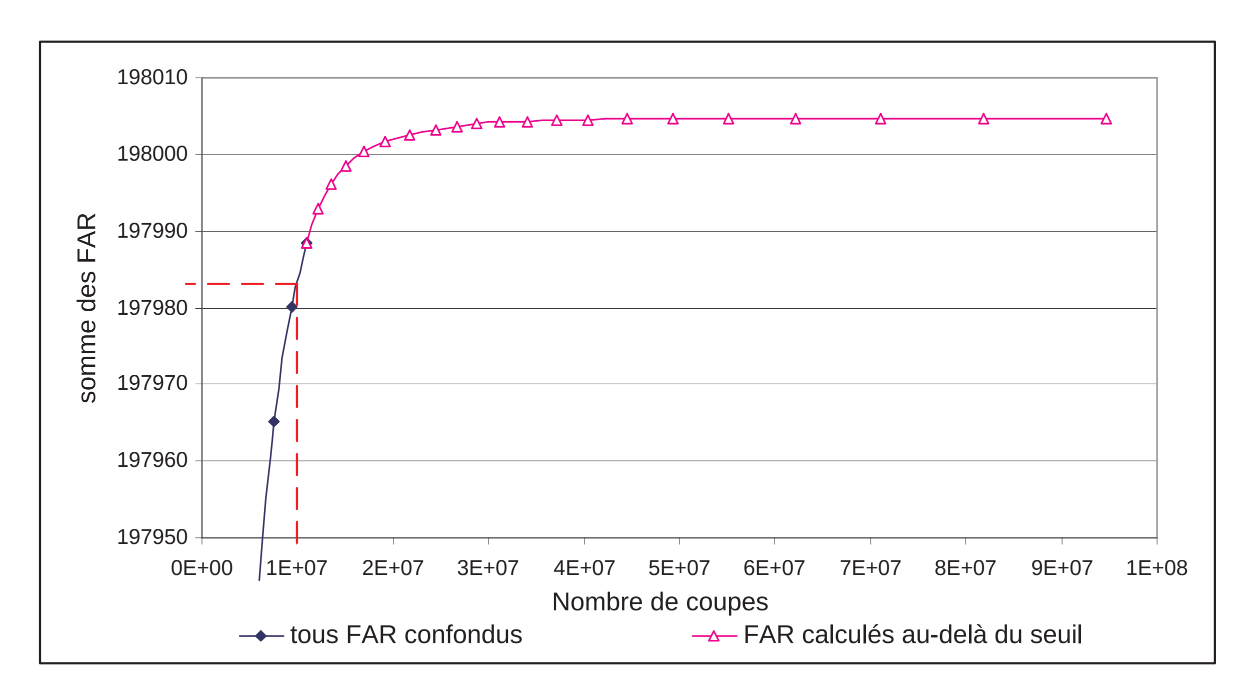


Fig. C.2 – *Valeur de la somme des FAR de tous les EB calculée en fonction du seuil de troncature pour le modèle EPR V10.01*